CA ARCserve® Central Virtual Standby

Guia do Usuário

r16

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA Technologies:

- CA ARCserve® Backup
- CA ARCServe® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Entrar em contato com a CA

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Links para suporte ao CA ARCserve Central Applications:

O CA Support online oferece um abrangente conjunto de recursos para solucionar seus problemas técnicos e fornece acesso fácil a importantes informações sobre o produto. Por meio do CA Support, você tem acesso fácil a consultas confiáveis que estão sempre disponíveis. Os links abaixo permitem acessar vários sites do CA Support disponíveis:

- **Entendendo o suporte --** O link abaixo fornece informações sobre programas de manutenção e ofertas de suporte, incluindo termos e condições, declarações, SLOs (Service-Level Objectives - Objetivos de Nível de Serviço) e horários de atendimento.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrando-se para obter suporte --** O link abaixo o direciona para o formulário de registro online do CA Support que é usado para ativar o suporte ao produto.

  https://support.ca.com/prodinfo//supportregistration

- **Acessando o Suporte técnico --** O link abaixo o direciona à página de suporte ao CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Alterações na documentação

Esta documentação inclui comentários do usuário, aprimoramentos, correções e outras alterações secundárias para ajudar a melhorar a utilização e a compreensão do produto ou da própria documentação.

As seguintes atualizações na documentação foram feitas desde a última versão GA desta documentação:

Update 6

- Diretivas de implantação (na página 39) atualizadas. Este tópico inclui agora uma observação indicando que você pode visualizar o status da implantação de diretivas na tela de lista Nó na coluna Diretivas.
- Atualizar nós (na página 48) atualizados. O tópico descreve como é possível atualizar vários nós simultaneamente usando as credenciais existentes ou especificando novas credenciais. Também é possível forçar o servidor para gerenciar os nós selecionados.
- Adicionar grupos de nós (na página 28) atualizados. Este tópico substitui o grupo de nó "Não atribuído" com "Nós sem uma diretiva" e substitui o grupo de nó "Sem grupo" com "Nós sem um grupo".
- Ligar máquinas virtuais no modo de espera virtual pelos instantâneos de ponto de recuperação (na página 85) atualizado. Esse tópico foi atualizado para incluir um novo botão chamado VM de espera na barra de ferramentas Ações do nó. Esse recurso permite ligar uma máquina virtual diretamente pelo aplicativo.

Update 5

- Atualizado para incluir comentários do usuário, aprimoramentos, correções e outras alterações secundárias para ajudar a melhorar a utilização o e a compreensão do produto ou da documentação.
- Adicionar grupos de nós (na página 28). Esse tópico foi atualizado para incluir os filtros Nome do grupo e Nome do nó.
- Atribuir nós a uma diretiva (na página 38). Esse tópico foi atualizado para incluir os filtros Nome do grupo e Nome do nó.
- Atualizar nós (na página 48). A atualização deste tópico inclui várias maneiras de atualizar diversos nós.
- Remover a atribuição de nós de diretivas (na página 64). Esse tópico foi atualizado para incluir os filtros Nome do grupo e Nome do nó.

Update 4

- Implantar diretivas (na página 39) atualizado para incluir mais informações sobre como o processo de implantação afeta os nós importados do Host-Based VM Backup.
- Pausar e retomar sinais de monitoramento atualizado para descrever como pausar e retomar sinais de monitoramento no servidor do Virtual Standby (na página 79) e diretamente no nó (na página 82).
- Pausar e retomar tarefas do Virtual Standby atualizado para descrever como pausar e retomar tarefas do Virtual Standby no servidor do Virtual Standby (na página 83) e diretamente no nó (na página 84).
- Restaurar dados de pontos de recuperação do CA ARCserve D2D (na página 102), Restaurar dados de cópias de arquivos do CA ARCserve D2D (na página 107), Restaurar dados usando a opção Localizar arquivos/pastas para restauração (na página 112) e Restaurar mensagens de email do Microsoft Exchange (na página 164) atualizados. Esses tópicos descrevem como restaurar dados usando a nova ação Restaurar na barra de ferramentas.
- Alterar o protocolo de comunicação do servidor (na página 172) adicionado. Este tópico descreve como alterar o protocolo de comunicação usado pelos componentes do CA ARCserve Central Applications de HTTP para HTTPS e de HTTPS para HTTP usando um arquivo em lote.

Índice

Capítulo 5: Solucionando problemas do CA ARCserve Central Virtual Standby 173

Capítulo 6: Aplicando práticas recomendadas 207

Capítulo 1: Introdução ao CA ARCserve Central Virtual Standby

Esta seção contém os seguintes tópicos:

Introdução

O CA ARCserve Central Applications combina as principais tecnologias de gerenciamento e proteção de dados com um ecossistema de aplicativos de destino que funcionam em uníssono para possibilitar proteção, cópia, movimentação e transformação de dados, no local e remotamente, em ambientes globais.

O CA ARCserve Central Applications é fácil de usar, gerenciar e instalar. Ele fornece às empresas controle automatizado de suas informações para tomarem decisões conscientes sobre o acesso, a disponibilidade e a segurança de seus dados, com base no valor comercial geral.

Entre os aplicativos oferecidos por CA ARCserve Central Applications está o CA ARCserve Central Virtual Standby. O CA ARCserve Central Virtual Standby integra-se com o CA ARCserve D2D e permite provisionar máquinas virtuais a partir de sessões de backup do CA ARCserve D2D. O aplicativo permite fazer o seguinte:

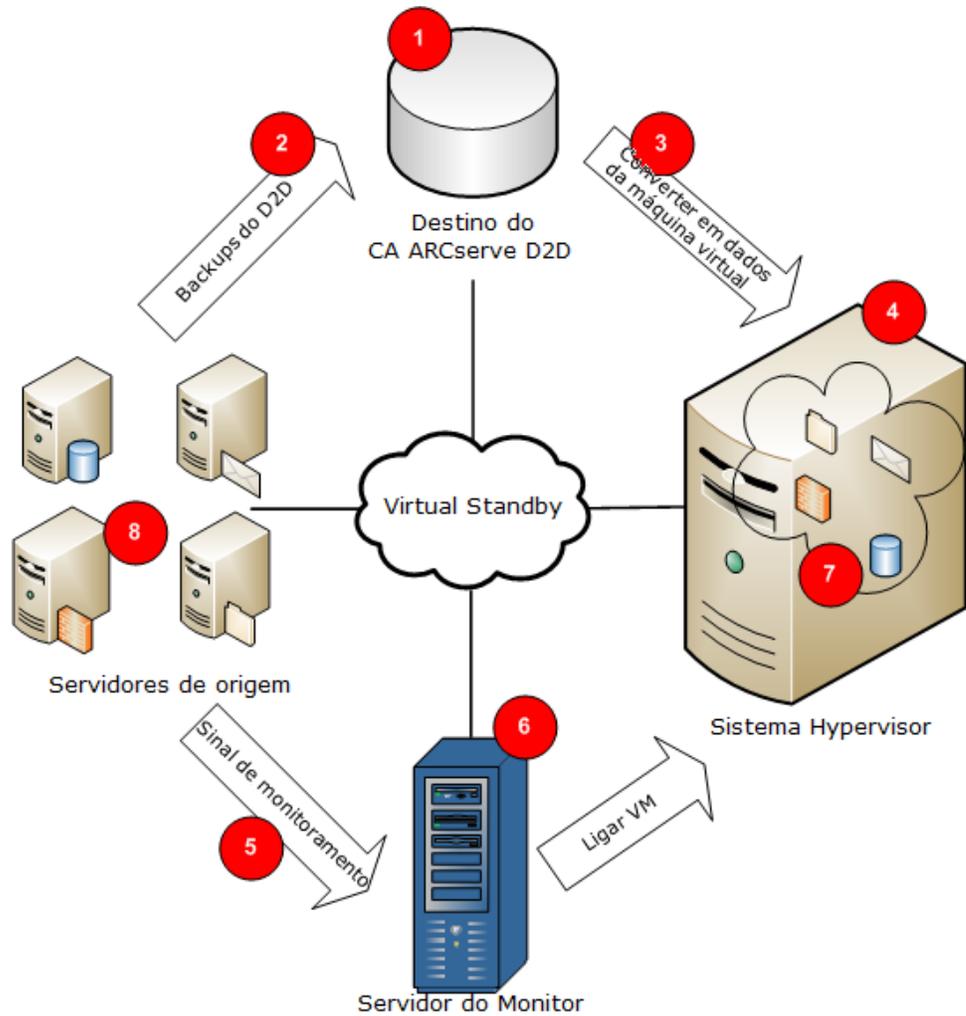
- Converter pontos de recuperação do CA ARCserve D2D que estão armazenados nos dispositivos de destino do CA ARCserve D2D em formatos VMware Virtual Disk (VMDK) ou Microsoft Virtual Hard Disk (VHD) com base em uma programação. A partir dos instantâneos do ponto de recuperação, você pode permitir que as máquinas virtuais funcionem como servidores de origem do CA ARCserve D2D caso seus servidores de origem falhem.
- Adicionar diretivas de conversão para servidores de origem do CA ARCserve D2D.
- Armazenar instantâneos do ponto de recuperação em máquinas virtuais com base em VMware ESX Server ou Hyper-V.
- Ligar as máquinas virtuais manual ou automaticamente se ocorrer uma situação de emergência.
- Recuperar dados dos instantâneos do ponto de recuperação para os servidores de origem originais ou alternativos (recuperações V2P).

Como o CA ARCserve Central Virtual Standby funciona

O Virtual Standby permite proteger os servidores de origem do CA ARCserve D2D funcionando em seu ambiente ao fazer o seguinte:

- Converter pontos de recuperação do CA ARCserve D2D que estão armazenados nos dispositivos de destino do CA ARCserve D2D em formatos VMware Virtual Disk (VMDK) ou Microsoft Virtual Hard Disk (VHD) com base em uma programação.
- Copiar os dados convertidos para um sistema de hypervisor.
- Criar instantâneos do ponto de recuperação a partir dos dados de VMDK ou VHD da máquina virtual.
- Monitorar a integridade do servidor de origem.
- Ligar máquinas virtuais automaticamente a partir dos instantâneos do ponto de recuperação após a detecção de uma emergência.

  Observação: o Virtual Standby pode ser configurado para ligar instantâneos do ponto de recuperação automática ou manualmente quando ocorrer um problema.
- Recuperar os dados da máquina virtual para o servidor de origem, depois que você corrigir os problemas no servidor de origem.

O diagrama a seguir ilustra esse processo:

O CA ARCserve D2D (1) cria pontos de recuperação no dispositivo de destino do CA ARCserve D2D (2) para os servidores de origem. O Virtual Standby converte os pontos de recuperação em formatos da máquina virtual (3) e armazena os dados como instantâneos do ponto de recuperação no sistema hypervisor (4).

O servidor de monitoramento (6) monitora a integridade dos servidores de origem. Se o servidor de monitoramento não puder detectar um sinal de monitoramento (5) a partir de um servidor de origem (8), o servidor de monitoramento é ligado em uma máquina virtual de pouco provisionamento (7) no sistema hypervisor (4), para funcionar como o servidor de origem com os dados contidos no instantâneo do ponto de recuperação mais recente. O CA ARCserve Central Virtual Standby cria uma partição da máquina virtual que seja do mesmo tamanho que o servidor de origem.

Depois de corrigir os problemas no servidor de origem, você pode recuperar o servidor de origem (8) para seu estado atual usando os dados (7) que estão armazenados na VM no sistema do hypervisor.

Observação: se quiser fazer backup da máquina virtual depois que ela for ligado, é possível implantar uma diretiva de backup do CA ARCserve D2D no computador virtual usando o Gerenciador do CA ARCserve Central Protection.

Biblioteca do CA ARCserve Central Applications

Os mesmos tópicos contidos no sistema de ajuda do CA ARCserve Central Applications também estão disponíveis como um Guia do Usuário em PDF. A versão mais recente deste guia e o sistema de ajuda podem ser acessados a partir da Biblioteca do CA ARCserve Central Applications.

Os arquivos de Notas da Versão do CA ARCserve Central Applications contém informações relacionadas aos requisitos do sistema, suporte ao sistema operacional, suporte à recuperação de aplicativos e outras informações que podem ser necessárias antes de instalar este produto. Além disso, estes arquivos contêm uma lista de problemas conhecidos os quais você deve saber antes de usar o CA ARCserve Central Applications. A versão mais recente de Notas da Versão pode ser acessada a partir da Biblioteca do CA ARCserve Central Applications.

Capítulo 2: Instalando o CA ARCserve Central Virtual Standby

Esta seção contém os seguintes tópicos:

Tarefas essenciais da instalação

Antes de instalar o CA ARCserve Central Virtual Standby, conclua as seguintes tarefas essenciais:

- Verifique se a última versão suportada do CA ARCserve D2D está instalado em:
  - Os servidores de origem que deseja proteger
  - O servidor designado para armazenar instantâneos de ponto de recuperação

    Observação: esse requisito se aplica somente aos servidores Hyper-V que estiverem configurados para monitorar a integridade dos nós (máquina física ou virtual) e para armazenar os instantâneos de ponto de recuperação para os nós.

  - O servidor designado para monitorar os servidores de origem

  Observação: se você instalou o Gerenciador do CA ARCserve Central Protection em seu ambiente de produção, é possível instalar o CA ARCserve D2D em nós remotos usando a Implantação do D2D. Para obter mais informações, consulte o Guia do Usuário do Gerenciador do CA ARCserve Central Protection.

- Em ambientes Hyper-V, verifique se o CA ARCserve D2D está instalado no sistema host Hyper-V. Em ambientes Hyper-V, os sistemas host Hyper-V funcionam como o local de armazenamento para instantâneos do ponto de recuperação e como o servidor de monitoramento.

- Em ambientes VMware, verifique se o CA ARCserve D2D está instalado no sistema proxy.

  Observação: em ambientes VMware, o armazenamento de dados do servidor ESX de destino funciona como o local de armazenamento para os instantâneos do ponto de recuperação. O sistema de proxy pode funcionar como o servidor de monitoramento.

- Revise o arquivo de Notas da versão. O arquivo de Notas da versão contém uma descrição de requisitos do sistema, sistemas operacionais suportados e uma lista de problemas conhecidos que existem nesta release.
- Verifique se o sistema atende aos requisitos mínimos de hardware e software necessários para a instalação do CA ARCserve Central Virtual Standby.
- Verifique se sua conta do Windows tem privilégios de administrador ou equivalente para instalar o software em computadores onde deseja instalar o CA ARCserve Central Virtual Standby.
- Verifique se a sua conta tem privilégios administrativos do VMware vCenter ou ESX e privilégios administrativos do Windows. É necessário atribuir a conta à função de licença global no sistema vCenter Server ou no sistema ESX Server para permitir que as operações do VDDK sejam concluídas com êxito.
- Verifique se você tem em mãos os nomes de usuário e senhas dos computadores em que você está instalando o CA ARCserve Central Virtual Standby.
- Verifique se você possui os nomes de host ou endereços IP de computadores que irão monitorar os computadores de origem que estejam em suas mãos.
- Verifique se possui os nomes de host ou endereços IP de computadores onde armazenará instantâneos do ponto de recuperação que estejam em suas mãos.
- Verifique se você tem todas as licenças necessárias para instalar o CA ARCserve Central Virtual Standby.
- Verifique se o número de release do CA ARCserve D2D é o mesmo do CA ARCserve Central Virtual Standby.

Considerações sobre a instalação

Antes de instalar o CA ARCserve Central Virtual Standby, revise as seguintes considerações de instalação:

- O pacote de instalação do CA ARCserve Central Applications instala um módulo chamado Servidor do CA ARCserve Central Applications. O servidor do CA ARCserve Central Applications é um módulo que é comum a todos os aplicativos CA ARCserve Central Applications. O módulo contém o serviço web, os binários e configurações que permitem que o CA ARCserve Central Applications se comunique com os outros.

  Ao instalar o CA ARCserve Central Applications, o pacote de instalação instala o módulo do servidor do CA ARCserve Central Applications antes de instalar os componentes do produto. Se for necessário aplicar um patch ao CA ARCserve Central Applications, ele atualizará o módulo antes de atualizar os componentes do produto.

- O CA ARCserve D2D instala o VDDK (VMware Virtual Disk Development Kit) em todos os computadores onde o CA ARCserve D2D foi instalado. Não é necessário fazer download e instalar o VDDK nos sistemas proxy do Virtual Standby.

  Se você deseja usar uma versão mais recente do VDDK, baixe e instale o VDDK e modifique o valor do Registro VDDKDirectory localizado em HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D para a pasta de instalação onde o VDDK está instalado.

  O local padrão para o VDDK é o seguinte:

  - **Sistema operacional X64**

    `c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit`

    Observação: descompacte o arquivo VDDK64.zip no diretório de instalação do VDDK para a pasta VDDK64.

    Por exemplo, c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\VDDK64

  - **Sistema operacional X86**

    `c:\Program Files\VMware\VMware Virtual Disk Development Kit`

- o CA ARCserve Central Virtual Standby não oferece suporte à criação de imagens de disco virtual em volumes compactados e volumes que foram criptografados pelo sistema de arquivos.

  Observação: esta limitação aplica-se apenas a hypervisors do Hyper-V.

- o CA ARCserve Central Virtual Standby não oferece suporte à proteção de máquinas virtuais VMware que são nomeadas usando os caracteres Unicode JIS2004.
- O CA ARCserve Central Virtual Standby não oferece suporte para proteção de máquinas virtuais que tenham um tamanho de disco maior do que dois terabytes.

Instalar o CA ARCserve Central Virtual Standby

O Assistente de instalação ajuda a orientá-lo durante todo o processo de instalação de um ou mais CA ARCserve Central Applications.

Observação: antes de instalar o aplicativo, consulte o arquivo Notas da versão e verifique se todas as tarefas descritas em Tarefas de pré-requisito foram concluídas.

Para instalar o CA ARCserve Central Virtual Standby

1. Baixe o pacote de instalação do CA ARCserve Central Applications para o computador no qual você deseja instalar o aplicativo e clique duas vezes no Arquivo de instalação.

   O pacote de instalação extrai seu conteúdo para o computador e, em seguida, a caixa de diálogo Componentes essenciais é aberta.

2. Clique em Instalar na caixa de diálogo Componentes essenciais.

   Observação: a caixa de diálogo Componentes essenciais será exibida somente se o programa de instalação não detectar os componentes essenciais instalados no computador.

   Depois que o programa de instalação instalar os componentes essenciais, a caixa de diálogo do Contrato de licença é aberta.

3. Preencha os campos necessários da caixa de diálogo Contrato de licença e clique em Avançar.

   A caixa de diálogo Configuração é aberta.

4. Na caixa de diálogo de Configuração, preencha o seguinte:

   - **Componentes -** especifique os aplicativos que você deseja instalar.

     Observação: se instalar esse aplicativo usando o conjunto do pacote de instalação, você poderá instalar vários aplicativos.

   - **Local -** aceite o local padrão da instalação ou clique em Procurar para especificar um local de instalação alternativo. O diretório padrão é o seguinte:

     `C:\Arquivos de programas\CA\ARCserve Central Applications\BIN`

   - **Informações do disco -** verifique se o disco rígido tem espaço livre suficiente para instalar os aplicativos.

   - **Nome do administrador do Windows -** especifique o nome de usuário da conta de administrador do Windows usando a seguinte sintaxe:

     `Domínio\Nome do usuário`

   - **Senha -** especifique a senha da conta do usuário.

   - **Especificar o número da porta -** especifique o número de porta que deseja usar para se comunicar com a interface do usuário baseada na web. Como prática recomendada, você deve aceitar o número de porta padrão. O número da porta padrão é o seguinte:

     `8015`

     Observação: se desejar especificar um outro número de porta, os números de porta disponíveis vão de 1024 a 65535. Para que você especifique um outro número de porta, verifique se o número de porta especificado está livre e disponível para uso. A instalação impede que você instale o aplicativo usando uma porta que não esteja disponível para uso.

   - **Usar HTTPS para a comunicação web** - especifique usar a comunicação HTTPS para a transmissão de dados. Essa opção não vem selecionada por padrão.

     Observação: a comunicação HTTPS (segura) fornece um nível maior de segurança do que a comunicação HTTP. O HTTPS é o protocolo de comunicação recomendado se você transmite informações confidenciais na rede.

- **Permitir que o programa de instalação registre como exceções os serviços/programas do CA ARCserve Central Applications no Firewall do Windows -** verifique se a caixa de seleção para essa opção está marcada. As exceções do firewall são necessárias para configurar e gerenciar o CA ARCserve Central Applications por meio de computadores remotos.

  Observação: para usuários locais, não é preciso registrar as exceções do firewall.

Clique em Avançar.

O processo de instalação é executado.

Depois que o processo de instalação for concluído, a caixa de diálogo Relatório de instalação é aberta.

5. A caixa de diálogo Relatório de instalação resume a instalação. Se deseja verificar se há atualizações para o aplicativo agora, clique em Verificar se há atualizações e clique em Concluir.

O aplicativo está instalado.

Desinstalar o CA ARCserve Central Virtual Standby

É possível desinstalar o aplicativo usando Programas e Recursos, localizado no Painel de Controle do Windows.

Siga estas etapas:

1. No menu Iniciar do Windows, clique em Iniciar e em Painel de controle.

   O Painel de controle do Windows é aberto.

2. No Painel de controle do Windows, clique na lista suspensa próxima a Exibir por e, em seguida, clique em Ícones grandes ou Ícones pequenos.

   Os ícones dos aplicativos no Painel de controle do Windows aparecem em um layout de grade.

3. Clique em Programas e Recursos.

   A janela Desinstalar ou alterar um programa é aberta.

4. Localizar e clique no aplicativo que deseja desinstalar.

   Clique com o botão direito do mouse no aplicativo e clique em Desinstalar no menu pop-up.

   Siga as instruções na tela para desinstalar o aplicativo.

O aplicativo será desinstalado.

Instalar o CA ARCserve Central Virtual Standby de modo silencioso

O CA ARCserve Central Applications permite instalar o CA ARCserve Central Virtual Standby de modo silencioso. O processo de instalação silenciosa elimina a necessidade de interação com o usuário. As etapas a seguir descrevem como instalar o aplicativo usando a linha de comando do Windows.

Para instalar o CA ARCserve Central Virtual Standby de modo silencioso

1. Abra a linha de comando do Windows no computador onde deseja iniciar o processo de instalação silenciosa.
2. Faça download do pacote de instalação de auto-extração do CA ARCserve Central Applications para o computador.

   Inicie o processo de instalação silenciosa usando a seguinte sintaxe da linha de comando:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR>
   -Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"
   ```

   Utilização:

   s

   Permite executar o pacote de arquivo executável no modo silencioso.

   v

   Permite especificar outras opções de linha de comando.

   q

   Permite instalar o aplicativo no modo silencioso.

   -Path:<INSTALLDIR>

   (Opcional) Permite especificar o caminho de instalação de destino.

   Exemplo:

   ```
   -Path:\"C:\Arquivos de Programas\CA\ARCserve Central Applications\"
   ```

   Observação: se o valor de INSTALLDIR tiver um espaço, coloque o caminho entre barras invertidas e aspas. Além disso, o caminho não pode terminar com um caractere de barra invertida.

   -Port:<PORT>

   (Opcional) Permite especificar o número da porta para comunicação.

   Exemplo:

   ```
   -Porta:8015
   ```

-U:<UserName>

Permite especificar o nome de usuário a ser usado para instalar e executar o aplicativo.

Observação: o nome de usuário deve ser uma conta administrativa ou uma conta com privilégios administrativos.

-P:<Password>

Permite especificar a senha para o nome de usuário.

-Products:<ProductList>

(Opcional) Permite especificar uma instalação do CA ARCserve Central Applications de modo silencioso. Se você não especificar um valor para o argumento, o processo de instalação silenciosa instalará todos os componentes do CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

Gerenciador do CA ARCserve Central Protection

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Todos os aplicativos CA ARCserve Central Applications

TODOS

Observação: os exemplos a seguir descrevem a sintaxe necessária para instalar um, dois, três ou todos os aplicativos CA ARCserve Central Applications silenciosamente:

```
-Products:<CMX64>
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:<ALL>
```

O aplicativo foi instalado de modo silencioso.

Desinstalar o CA ARCserve Central Virtual Standby de modo silencioso

O CA ARCserve Central Applications permite desinstalar o CA ARCserve Central Virtual Standby de modo silencioso. O processo de instalação silenciosa elimina a necessidade de interação com o usuário. As etapas a seguir descrevem como desinstalar o aplicativo usando a linha de comando do Windows.

Siga estas etapas:

1. Efetue logon no computador de onde deseja desinstalar o aplicativo.

   Observação: é necessário efetuar logon usando uma conta administrativa ou uma conta com privilégios administrativos.

2. Abra a linha de comando do Windows e execute o seguinte comando para iniciar o processo de desinstalação silenciosa:

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>
   ```

   Ou

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /ALL
   ```

   Exemplo: a sintaxe a seguir permite desinstalar o CA ARCserve Central Virtual Standby silenciosamente.

   ```
   "%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED4835-964B-484B-A395-E2DF12E6F73D}
   ```

Utilização:

<INSTALLDIR>

Permite especificar o diretório no qual o aplicativo está instalado.

Observação: execute a sintaxe que corresponde à arquitetura do sistema operacional do computador.

<ProductCode>

Permite especificar o aplicativo a ser desinstalado silenciosamente.

Observação: o processo de desinstalação silenciosa permite instalar um ou mais aplicativos CA ARCserve Central Applications. Use os seguintes códigos de produtos para desinstalar o CA ARCserve Central Applications de modo silencioso:

CA ARCserve Central Host-Based VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

Gerenciador do CA ARCserve Central Protection

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

O aplicativo é desinstalado de modo silencioso.

Capítulo 3: Introdução ao CA ARCserve Central Virtual Standby

As seções a seguir descrevem como configurar o CA ARCserve Central Virtual Standby para proteger os nós do CA ARCserve D2D.

Observação: antes de concluir as configurações descritas nesta seção, verifique se toda as tarefas de pré-requisito dsainstalação (na página 15) foram concluídas.

Esta seção contém os seguintes tópicos:

Verifique se o servidor do CA ARCserve Central Virtual Standby pode se comunicar com os nós

Observação: esta é uma etapa opcional para configurar o CA ARCserve Central Virtual Standby para proteger os nós.

Para garantir que o CA ARCserve Central Virtual Standby poderá implantar diretivas para nós e protegê-los, verifique se o servidor do Virtual Standby e os nós que deseja proteger podem se comunicar uns com os outros usando seus nomes de host.

Verifique se o servidor do CA ARCserve Central Virtual Standby pode se comunicar com os nós

1. No servidor do CA ARCserve Central Virtual Standby, digite o comando ping para os nós que deseja proteger usando sues respectivos nomes de host.
2. Nos nós que deseja proteger, execute o servidor do CA ARCserve Central Virtual Standby usando o nome do host do servidor.

Efetuar logon no CA ARCserve Central Virtual Standby

Pode-se efetuar logon no CA ARCserve Central Virtual Standby diretamente a partir do computador em que o aplicativo está instalado ou a partir de um computador remoto usando um navegador suportado. Para obter uma lista completa dos navegadores suportados, consulte as *Notas da versão do CA ARCserve Central Virtual Standby*.

Para efetuar logon no CA ARCserve Central Virtual Standby

1. Execute uma das opções a seguir:

   - Se você estiver conectado ao servidor onde o CA ARCserve Central Virtual Standby está instalado, inicie o aplicativo de seus arquivos de programa.

     Uma janela do navegador é aberta e a tela de logon do CA ARCserve Central Virtual Standby aparece.

     Preencha os seguintes campos na tela de logon:

     – Nome de usuário

     – Senha

     Clique em Efetuar logon.

   - Caso não esteja conectado ao servidor onde o CA ARCserve Central Virtual Standby está instalado, abra uma janela do navegador e especifique o seguinte URL na barra de endereços:

     ```
     http://<Nome do servidor do CA ARCserve Central Applications>:<Número da porta>/virtualstandby/
     ```

     Observação: pode-se especificar o nome do host ou o endereço IP do servidor quando o CA ARCserve Central Virtual Standby está instalado. A porta padrão é 8015.

     Pressione Enter.

     Uma janela do navegador é aberta e a tela de logon do CA ARCserve Central Virtual Standby aparece.

     Preencha os seguintes campos na tela de logon:

     – Nome de usuário

     – Senha

     Clique em Efetuar logon.

   Você está conectado no CA ARCserve Central Virtual Standby e a página inicial é exibida.

Adicionar nós por endereço IP ou nome de nó

O Virtual Standby permite adicionar nós com base no endereço IP ou no nome do nó. Adicione os nós de origem do CA ARCserve D2D que deseja proteger.

Para adicionar nós por endereço IP ou nome de nó

1. Na página inicial, selecione Nó na Barra de navegação.

   A tela Nó é exibida.

2. Na barra de ferramentas Nó, clique em Adicionar e, em seguida, clique em Adicionar nó por IP/nome no menu pop-up.

   A caixa de diálogo Adicionar nó por IP/Nome é aberta.

3. Preencha os campos abaixo na caixa de diálogo Adicionar nó por do IP/Nome:

   - **IP/Nome do nó** - permite especificar o endereço IP ou o nome do nó.
   - **Descrição** - permite especificar uma descrição para o nó.
   - **Nome de usuário -** permite especificar o nome de usuário necessário para efetuar logon no nó.
   - **Senha -** permite especificar a senha necessária para fazer logon no nó.

   Clique em OK.

4. (Opcional) Se o nó recém-adicionado não aparecer na lista de nós, clique em Atualizar na barra de ferramentas Nó.

A caixa de diálogo Adicionar nó por IP/Nome é fechada e o nó é adicionado.

Adicionar grupos de nós

Os grupos de nós permitem gerenciar um grupo de computadores de origem do CA ARCserve D2D de acordo com características comuns. Por exemplo, é possível definir grupos de nós classificados pelo departamento que eles suportam: contabilidade, marketing, jurídico, recursos humanos e assim por diante.

O aplicativo contém os seguintes grupos de nós:

- **Grupos padrão:**
  - **Todos os nós -** contém todos os nós associados ao aplicativo.
  - **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
  - **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
  - **Servidor SQL -** contém todos os nós associados ao aplicativo e o Microsoft SQL Server está instalado no nó.
  - **Exchange -** contém todos os nós associados ao aplicativo e o Microsoft Exchange Server está instalado no nó.

  Observação: não é possível modificar ou excluir os grupos de nós padrão.
- **Grupos personalizados--**contém grupos de nós personalizados.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.
2. Clique em Adicionar na barra de ferramentas Grupo de nós.

   A caixa de diálogo Adicionar grupo é aberta e nós aparecem na lista de Nós disponíveis.
3. Especifique um nome de grupo para o grupo de nós.
4. Preencha os campos abaixo na caixa de diálogo Adicionar grupo:
   - **Grupo--**selecione o nome do grupo que contém os nós que deseja atribuir.
   - **Filtro Nome do nó--**permite filtrar os nós disponíveis com base em critérios comuns.

     Observação: o filtro Nome do nó suporta o uso de caracteres curinga.

     Por exemplo, usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc. Para limpar os resultados do filtro, clique em X no campo Filtro.

5. Para adicionar nós ao grupo de nós, selecione um ou mais nós que deseja adicionar e clique na seta à direita.

   Os nós passam da lista Nós disponíveis para a lista Nós selecionados e são atribuídos ao grupo de nós.

   Observação: para selecionar e mover todos os nós do grupo atual, clique na seta dupla à direita.

6. (Opcional): para mover todos os nós da lista Nós selecionados para a lista Nós disponíveis, clique na seta simples à esquerda.

   Observação: para selecionar e mover todos os nós do grupo atual, clique na seta dupla à esquerda.

7. Clique em OK.

O Grupo de nós é adicionado.

Especificar o sistema ESX Server ou vCenter Server para nós do VMware

Observação: o procedimento a seguir se aplica somente a nós de origem da máquina virtual com base em VMware.

Em diversas implementações com base no VMware, o Virtual Standby pode não detectar nós de origem configurados como máquinas virtuais que residem em sistemas ESX Server e vCenter Server. Este comportamento evita que o Virtual Standby aplique a licença correta aos nós, implante diretivas para os nós e execute tarefas de conversão.

O procedimento a seguir permite especificar o nome do host ou o endereço IP do sistema ESX Server ou vCenter Server onde os nós residem. Depois de concluir o procedimento, o Virtual Standby poderá detectar, aplicar licenças, implantar diretivas e executar tarefas de conversão dos nós que deseja proteger. Se houver várias máquinas virtuais residindo no sistema ESX Server ou vCenter Server que atuam como um nó de origem, o procedimento permite consumir uma licença para todos os nós, ajudando a reduzir o custo geral da proteção dos nós de origem.

Para especificar o sistema ESX Server ou vCenter Server para nós do VMware

1. Efetue logon no aplicativo.

   Na Barra de navegação na página inicial, clique em Nó.

   A tela Nó é exibida.

2. Na barra de Grupos, clique no grupo Todos os nós ou clique no nome de grupo contendo o nó que você deseja atualizar.

   Os nós associados ao grupo aparecem na lista de nós.

3. Clique no nó que deseja atualizar e, em seguida, clique em Especificar servidor ESX no menu pop-up.

   A caixa de diálogo Especificar servidor de ESX é aberta.

   Observação: uma mensagem de erro será exibida se o aplicativo detectar que o VMware Tools não está instalado na máquina virtual gerenciada por um sistema ESX Server ou vCenter Server, a máquina virtual residir em um sistema Hyper-V ou o nó detectado não for uma máquina virtual.

4. Preencha os campos abaixo na caixa de diálogo Especificar servidor ESX:

   - Host ESX/vCenter

     Observação: especifique o nome do host ou o endereço IP do sistema ESX Server ou vCenter Server.

   - Nome de usuário
   - Senha
   - Porta

     Observação: a porta padrão de comunicação é 443. Se o nó se comunica com o sistema ESX Server ou vCenter Server usando um número de porta diferente, especifique o número da porta que será usado.

   - Protocolo

     Observação: o protocolo padrão de comunicação é HTTPS. Se o nó se comunica com o sistema ESX Server ou vCenter Server usando HTTP, clique em HTTP.

   Clique em OK.

O sistema ESX Server ou vCenter Server foi atribuída ao nó.

Criar diretivas

O Virtual Standby permite definir diretivas de conversão personalizadas que você atribui a nós do CA ARCserve D2D.

Observação: para criar diretivas, o CA ARCserve D2D deve estar instalado no servidor de monitoramento.

Para criar diretivas

1. Efetue logon no servidor do Virtual Standby e abra o Virtual Standby.

   Na barra de navegação na página inicial, clique em Diretivas.

   A janela Diretiva é aberta.

2. Clique em Novo na barra de ferramentas de Diretivas.

   A caixa de diálogo Nova diretiva é aberta.

3. No campo Nome da diretiva, especifique um nome para a diretiva.

   Clique na guia Virtual Standby.

   As opções Servidor de virtualização, Máquina virtual e Configurações substitutas são exibidas.

4. Clique em Servidor de virtualização.

   As opções do Servidor de virtualização são exibidas.

5. Preencha as seguintes opções do servidor de virtualização:

   Sistemas VMware:

   - **Tipo de virtualização -** clique em VMware.
   - **Host do ESX/vCenter--**especifique o nome de host do sistema ESX ou vCenter Server.
   - **Nome de usuário** - especifique o nome de usuário necessário para fazer logon no sistema VMware.

     Observação: a conta especificada deve ser uma conta administrativa ou uma conta com privilégios administrativos no sistema ESX ou vCenter Server.
   - **Senha -** especifique a senha para o nome do usuário necessária para fazer logon no sistema VMware.
   - **Protocolo -** especifique HTTP ou HTTPS, dependendo do protocolo que você deseja usar para a comunicação entre o nó do CA ARCserve D2D de origem e o servidor de monitoramento.
   - **Porta -** especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o servidor de monitoramento.
   - **Nó do ESX -** os valores neste campo variam de acordo com o valor especificado no campo Host do ESX/vCenter:
     - **Sistemas ESX Server -** ao especificar um sistema ESX Server no campo Host do ESX/vCenter, esse campo exibe o nome do host do sistema ESX Server.
     - **Sistemas vCenter Server -** ao especificar um sistema vCenter Server no campo Host do ESX/vCenter, esse campo permite especificar (a partir de uma lista suspensa) o sistema ESX Server que deseja associar a tal diretiva.

- **Servidor de monitoramento** - especifique o nome do host do servidor do qual deseja obter o status do servidor de origem monitorado.

  Observação: o servidor de monitoramento pode ser qualquer computador físico ou máquina virtual desde que o servidor não esteja funcionando como o servidor proxy para uma implementação do CA ARCserve Central Host-Based VM Backup.

- **Nome de usuário** - especifique o nome de usuário necessário para fazer logon no sistema de monitoramento.
- **Senha -** especifique a senha para o nome do usuário necessária para fazer logon no servidor de monitoramento.
- **Protocolo -** especifique HTTP ou HTTPS, dependendo do protocolo que você deseja usar para a comunicação entre o servidor CA ARCserve Central Virtual Standby e o sistema do ESX Server (servidor de monitoramento).
- **Porta -** especifique a porta que você deseja usar para a transferência de dados entre o servidor CA ARCserve Central Virtual Standby e o sistema do ESX Server (servidor de monitoramento).
- **Usar o servidor de monitoramento como proxy para a transferência de dados -** especifique essa opção para permitir que o servidor de monitoramento copie os dados de conversão do nó de origem do CA ARCserve D2D para o armazenamento de dados do ESX Server. Com essa opção ativada, o Virtual Standby transfere os dados de conversão do nó de origem para o armazenamento de dados do ESX Server usando a comunicação de canal de fibra, que é mais rápido do que usar a comunicação LAN, para transferência de dados.

  Observação: a opção Usar o servidor de monitoramento como proxy para a transferência de dados fica ativada por padrão. É possível desativar essa opção para permitir que o servidor de origem do CA ARCserve D2D copie os dados de conversão diretamente para o armazenamento de dados no sistema ESX Server.

Sistemas Hyper-V:

- **Tipo de virtualização -** clique em Hyper-V.

  Observação: quando você clica em Hyper-V, as opções de monitoramento não estão acessíveis. Isso acontece porque o servidor Hyper-V assume a função do servidor de monitoramento.

- **Nome do Host Hyper-V** - especifique o nome do host do sistema Hyper-V.
- **Nome de usuário** - especifique o nome de usuário necessário para fazer logon no sistema Hyper-V.

  Observação: a conta especificada deve ser uma conta administrativa ou uma conta com privilégios administrativos no sistema Hyper-V.

- **Senha -** especifique a senha para o nome do usuário necessária para fazer logon no sistema Hyper-V.
- **Porta -** especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o servidor de monitoramento.
- **Servidor de monitoramento** - especifique o nome do host do servidor do qual deseja obter o status do servidor de origem monitorado.
- **Nome de usuário** - especifique o nome de usuário necessário para fazer logon no sistema de monitoramento.
- **Senha -** especifique a senha para o nome do usuário necessária para fazer logon no servidor de monitoramento.
- **Protocolo -** especifique HTTP ou HTTPS, dependendo do protocolo que você deseja usar para a comunicação entre o servidor CA ARCserve Central Virtual Standby e o sistema do Hyper-V Server (servidor de monitoramento).
- **Porta -** especifique a porta que você deseja usar para a transferência de dados entre o servidor CA ARCserve Central Virtual Standby e o sistema do Hyper-V Server (servidor de monitoramento).

Clique em Máquina virtual.

As opções de máquina virtual são exibidas.

6. Preencha as seguintes opções de máquina virtual:

   Sistemas VMware:

   Aplique as opções a seguir da máquina virtual para sistemas VMware:

   - **Prefixo do nome da VM--**especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual do sistema ESX Server.

     Valor padrão: CAVM_

   - **Pool de recursos da VM -** especifique o nome do pool de recursos no qual a máquina virtual em modo de espera será agrupada.

   - **Contagem de CPU -** especifique a contagem de CPU mínima e máxima suportada pela máquina virtual em modo de espera.

   - **Memória -** especifique a quantidade total de RAM (em MB) a ser alocada para a máquina virtual em modo de espera.

     Observação: a quantidade de RAM especificada deve ser um múltiplo de dois.

   - **Armazenamento de dados da VM -** especifique o local onde deseja armazenar os dados de conversão.

     – **Especificar um armazenamento de dados para todos os discos virtuais -** permite que o aplicativo copie todos os discos relacionados à máquina virtual para um armazenamento de dados.

     – **Especificar um armazenamento de dados para cada disco virtual -** permite que o aplicativo copie informações relacionadas ao disco da máquina virtual para o armazenamento de dados correspondente.

   - **Redes da VM -** permite definir NICs, redes virtuais e os caminhos que o sistema ESX Server usa para se comunicar com as máquinas virtuais.

     – **Especificar um tipo de adaptador de rede para cada NIC e conectar o adaptador de rede à seguinte rede virtual -** permite definir como mapear o NIC virtual à rede virtual. Especifique essa opção quando a máquina virtual contiver NICs virtuais e uma rede virtual.

     – **Especificar um tipo de adaptador de rede e uma rede virtual para cada NIC -** permite definir o nome da rede virtual que deseja que o NIC use para se comunicar.

Sistemas Hyper-V:

Aplique as opções a seguir da máquina virtual para sistemas Hyper-V:

- **Configurações básicas da VM -** conclua as seguintes configurações básicas:
  - **Prefixo do nome da VM -** especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual do sistema Hyper-V.

    Valor padrão: CAVM_

    Contagem de CPU - especifique a contagem de CPU mínima e máxima suportada pelo sistema virtual no modo de espera.
  - **Memória -** especifique a quantidade total de RAM (em MB) a ser alocada para a máquina virtual em modo de espera.

    Observação: a quantidade de RAM especificada deve ser um múltiplo de quatro.
- **Caminho da VM -** especifique uma das seguintes opções de caminho de VM:
  - **Especificar um caminho para todos os discos virtuais -** especifique o local no servidor Hyper-V onde deseja armazenar os dados de conversão.
  - **Especificar um caminho para cada disco virtual -** especifique o local no servidor Hyper-V onde deseja armazenar os dados de conversão para cada disco virtual.

  Observação: o CA ARCserve Central Virtual Standby não oferece suporte à criação de imagens de disco virtual (arquivos VHD) em volumes compactados e volumes que foram criptografados pelo sistema de arquivos. Se o caminho especificado residir em volumes compactados ou criptografados do Hyper-V, o Virtual Standby impede a criação da diretiva.
- **Rede da VM -** permite definir NICs, redes virtuais e os caminhos que o sistema Hyper-V Server usa para se comunicar com as máquinas virtuais. Especifique uma das seguintes opções e preencha os campos solicitados.
  - **Especificar um tipo de adaptador de rede para cada NIC e conectar o adaptador de rede à seguinte rede -** permite definir como mapear a NIC virtual para a rede virtual. Especifique essa opção quando a máquina virtual contiver NICs virtuais e uma rede virtual.
  - **Especificar um tipo de adaptador de rede e uma rede virtual para cada NIC -** permite definir o nome da rede virtual que deseja que o NIC use para se comunicar.

Clique em Configurações substitutas.

As opções de Configurações substitutas são exibidas.

7. Preencha as seguintes opções de Configurações substitutas:

   Recuperação:

   Selecione um dos seguintes métodos:

   - **Iniciar a máquina virtual manualmente -** permite ligar e configurar manualmente máquinas virtuais quando o servidor de origem falha ou interrompe a comunicação. Especifique esta opção quando preferir analisar a causa da falha antes de configurar as máquinas virtuais e permitir aos servidores funcionarem como servidores de origem.
   - **Iniciar a máquina virtual automaticamente -** permite ligar e configurar automaticamente máquinas virtuais quando o servidor de origem falha ou interrompe a comunicação. Especifique esta opção quando deseja permitir que as máquinas virtuais parem de funcionar como servidores de origem imediatamente após os servidores de origem falharem ou interromperem a comunicação.

   Observação: a opção de recuperação padrão é Iniciar manualmente a máquina virtual.

   Propriedades do sinal de monitoramento:

   - **Tempo limite--**especifique o tempo que o servidor de monitoramento deve aguardar um sinal de monitoramento antes de ligar o instantâneo de um ponto de recuperação.
   - **Frequência--**especifique a frequência com que o servidor de origem fará a comunicação dos sinais de monitoramento com o servidor do monitor.

     Exemplo: o valor de tempo limite especificado é 60. O valor de frequência especificado é 10. O servidor de origem comunicará sinais de monitoramento em intervalos de 10 segundos. Se o servidor de monitoramento não detectar um sinal de monitoramento em 60 segundos do último sinal detectado, ele ligará a máquina virtual usando o instantâneo do ponto de recuperação mais recente.

   Clique na guia Preferências.

   A janela de opções de Alertas por emails é exibida.

8. Preencha as seguintes opções de Alertas por email:

   - **Sinal de monitoramento faltando para a máquina de origem -** o Virtual Standby envia notificações de alerta quando o servidor de monitoramento não detecta um sinal de monitoramento no servidor de origem.
   - **VM ligada para a máquina de origem configurada para ser ligada automaticamente -** o Virtual Standby envia notificações de alerta quando ele liga uma máquina virtual que foi configurada para ligar automaticamente quando um sinal de monitoramento não é detectado.
   - **Sinais de monitoramento ausentes para a máquina de origem configurada para ser ligada manualmente -** o Virtual Standby envia notificações de alerta quando ele não detecta um sinal de monitoramento de um servidor de origem que não esteja configurado para ligar automaticamente.
   - **Espaço livre de armazenamento da VM abaixo de -** o Virtual Standby envia notificações de alerta quando detecta espaço livre em disco insuficiente no caminho definido pelo HyperVisor. A detecção ocorre quando a quantidade de espaço livre em disco é menor do que o limite definido pelo usuário. O limite máximo pode ser representado como um valor absoluto (em MB) ou uma porcentagem da capacidade do volume.
   - **Erros/falhas/paralisação no Virtual Standby -** o Virtual Standby envia notificações de alerta quando detecta um erro que ocorreu durante o processo de conversão.
   - **Operação do Virtual Standby realizada com êxito -** o Virtual Standby envia notificações de alerta quando detecta que uma máquina virtual foi ligada com êxito.
   - **O Hypervisor não está acessível -** o Virtual Standby envia notificações de alerta quando detecta que ele não pode se comunicar com o sistema ESX Server ou com o sistema Hyper-V.
   - **Falha na licença -** especifica que o Virtual Standby deve enviar notificações de alerta quando detectar problemas de licenciamento em servidores do Virtual Standby, servidores de origem e servidores de monitoramento.
   - **O Virtual Standby não foi iniciado com êxito a partir do instantâneo do ponto de recuperação -** o Virtual Standby envia notificações de alerta quando detecta que uma máquina virtual não foi ligada automaticamente e a opção de início automático da recuperação de substituição da máquina virtual é especificada.

   Clique em Salvar.

A diretiva é salva.

Atribuir nós a uma diretiva

Para criar instantâneos de pontos de recuperação, é necessário atribuir diretivas de conversão do modo de espera virtual nos nós do CA ARCserve D2D que deseja proteger.

Observação: não é possível aplicar mais de uma diretiva a um nó.

Siga estas etapas:

1. Efetue logon no servidor do Virtual Standby e abra o Virtual Standby.

   Na barra de navegação na página inicial, clique em Diretivas para abrir a tela Diretivas.

2. Na lista de diretivas, clique na diretiva para a qual deseja atribuir nós.

   Informações detalhadas sobre a diretiva especificada são exibidas na guia Detalhes de diretiva e na guia Atribuição de diretiva.

3. Clique na guia Detalhes da diretiva para exibir informações detalhadas sobre a diretiva.

   (Opcional) Clique em Editar na barra de ferramentas para editar as configurações atuais da diretiva.

   Observação: para obter mais informações, consulte Editar diretivas (na página 56).

4. Clique na guia Atribuição de diretiva.

   Clique em Atribuir e remover a atribuição na guia Atribuição de diretiva.

   A caixa de diálogo Atribuir/remover atribuição de diretiva é aberta.

5. Especifique os seguintes campos da caixa de diálogo Atribuir/remover a atribuição de diretiva:

   - **Grupo--**selecione o nome do grupo que contém a diretiva que deseja atribuir.
   - **Filtro Nome do nó--**permite filtrar os nós disponíveis com base em critérios comuns.

   Observação: o campo Filtro permite o uso de caracteres curinga.

   Exemplos:

   - Usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc.
   - Usar *.123 permite filtrar todos os nós que contenham .123 no endereço IP.

   Observação: para limpar os resultados do filtro, clique no x no campo Filtro.

6. Execute uma das seguintes ações:

   - **Atribuir um nó--**na lista Nós disponíveis, localize o nó que você deseja atribuir à diretiva.

     Clique na seta única à direita.

     O nó é movido da lista de nós disponíveis para a lista de nós selecionados.

   - **Atribuir nós--**na lista de nós disponíveis, clique na seta dupla à direita.

     Todos os nós são movidos da lista de nós disponíveis para a lista de nós selecionados.

   Clique em OK.

Os nós são atribuídos à diretiva.

Implantar diretivas

Depois de criar uma diretiva, é necessário atribuir nós a uma diretiva (na página 38) e, em seguida, implantá-la.

O seguinte comportamento aplica-se ao processo de implantação da diretiva:

- O processo de implantação de diretiva falhará nas seguintes condições:
  - A função do Windows Server 2008 Hyper-V está instalada no servidor de origem (nó) do CA ARCserve D2D.
  - O nó do CA ARCserve D2D foi importado do CA ARCserve Central Host-Based VM Backup. A função do Windows Hyper-V está ativada no sistema proxy do Host-Based VM Backup e o sistema proxy de backup é especificado como o destino do Virtual Standby.
- O CA ARCserve Central Virtual Standby não pode ligar automaticamente máquinas virtuais que foram adicionadas de servidores do CA ARCserve Central Host-Based VM Backup. Como resultado, ao implantar diretivas que contenham um método de recuperação definido como Iniciar a máquina virtual automaticamente para nós protegidos pelo Host-Based VM Backup (na página 30), o Virtual Standby altera o valor do método de recuperação para Iniciar a máquina virtual manualmente (na página 30).

Siga estas etapas:

1. Efetue logon no servidor do Virtual Standby e abra o Virtual Standby.

   Na barra de navegação na página inicial, clique em Diretivas para abrir a tela Diretivas.

2. Na lista de diretivas, clique na diretiva que deseja implantar.

   Informações detalhadas sobre a diretiva especificada são exibidas na guia Detalhes de diretiva e na guia Atribuição de diretiva.

3. Clique na guia Detalhes da diretiva para exibir informações detalhadas sobre a diretiva.

   (Opcional) Clique em Editar na barra de ferramentas para editar as configurações atuais da diretiva.

   Observação: para obter mais informações, consulte Editar diretivas (na página 56).

4. Clique na guia Atribuição de diretiva.

   As informações detalhadas sobre os nós atribuídos à diretiva são exibidas.

   (Opcional) Clique em Atribuir e Remover atribuição na barra de ferramentas para atribuir ou remover a atribuição de nós para a diretiva.

   Observação: para obter mais informações, consulte o tópico Atribuir nós a diretivas (na página 38) ou Remover atribuição de nós de diretivas (na página 64).

5. Clique em Implantar agora na barra de ferramentas.

   A mensagem de confirmação Implantar agora é exibida.

6. Clique em OK.

A diretiva é implantada.

Observação: também é possível exibir o status de implantação da diretiva para o determinado nó na tela Nó na coluna Diretiva.

Capítulo 4: Usando o CA ARCserve Central Virtual Standby

Esta seção contém os seguintes tópicos:

Efetuar logon em nós do CA ARCserve D2D

Na página inicial do Virtual Standby, você pode fazer logon nos nós do CA ARCserve D2D.

Para fazer logon em nós do CA ARCserve D2D

1. Abra o aplicativo e clique em Nós na Barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

Você está conectado ao nó do CA ARCserve D2D.

Observação: a primeira vez que efetuar logon no nó do CA ARCserve D2D, uma página HTML pode se abrir exibindo uma mensagem de aviso. Isso pode ocorrer quando estiver usando o Internet Explorer. Para corrigir esse comportamento, feche o Internet Explorer e repita a etapa 3. Assim, será possível fazer logon no nó do CA ARCserve D2D com êxito.

Efetuar logon nos servidores de monitoramento

O Virtual Standby permite efetuar logon diretamente no servidor que está monitorando os nós de origem do CA ARCserve D2D. No servidor de monitoramento, é possível executar tarefas de manutenção e exibir informações sobre a integridade dos servidores de origem que o servidor de monitoramento está monitorando. É possível distinguir entre os nós do CA ARCserve D2D e os servidores de monitoramento por meio dos ícones a seguir:

Ícone de Servidor de monitoramento:

Ícone de nó do CA ARCserve D2D:

Para efetuar logon nos servidores de monitoramento

1. Efetue logon no servidor do Virtual Standby e abra o Virtual Standby.

   Na barra de navegação na página inicial, clique em Nós.

   A tela Nós é aberta.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Siga um destes procedimentos:

   - Se você souber o endereço IP ou nome de host do servidor de monitoramento, procure e clique no servidor de monitoramento no qual deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.
   - Se você souber o endereço IP ou nome de host do servidor de monitoramento, procure e clique no nó do CA ARCserve D2D no qual deseja efetuar logon e, em seguida, clique em Efetuar logon no servidor do monitor no menu pop-up.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

Você está conectado ao servidor de monitoramento.

Tarefas de manutenção do nó

O Virtual Standby permite usar vários métodos para adicionar nós:

- Adicionar nós por endereço IP ou nome de nó (na página 27).
- Importar nós de um arquivo (na página 44).

  Observação: este método permite importar vários nós de uma lista de nós em um arquivo separado por vírgulas.
- Adicionar nós de servidores CA ARCserve Central Host-Based VM Backup. (na página 46)

  Observação: este método permite importar nós de uma máquina virtual que estejam protegidos pelo aplicativo CA ARCserve Central Host-Based VM Backup.

Além disso, você pode executar as seguintes tarefas de gerenciamento do nó.

- Atualizar nós (na página 48).
- Excluir nós (na página 50).

Importar nós de um arquivo

O CA ARCserve Central Virtual Standby permite importar vários nós de um arquivo. Você pode importar os nós de um arquivo de texto com valores separados por vírgulas (.txt) ou de uma planilha (.CSV).

O aplicativo permite importar até 100 nós de um arquivo. Se o arquivo contém mais de 100 nós, o aplicativo importa apenas os primeiros 100 nós. Se você precisar adicionar mais de 100 nós, importe 100 usando um arquivo e, em seguida, adicione os nós restantes manualmente.

Observação: para obter informações sobre como adicionar nós manualmente, consulte Adicionar nós por endereço IP ou nome de nó. (na página 27)

Para importar nós de um arquivo

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, selecione Nó.

   A tela Nó é exibida.

2. Na barra de ferramentas Nó, clique em Adicionar e, em seguida, clique em Importar nós do arquivo no menu pop-up.

   A caixa de diálogo Selecionar nós é aberta.

3. Clique em Procurar para especificar o arquivo que contém os nós que você deseja importar.

   Observação: é possível especificar um arquivo de valores separados por vírgula (CSV) ou um arquivo de texto que contenha valores separados por vírgula.

   Clique em Carregar.

   Os nomes de nó e os nomes de usuário correspondentes são exibidos na caixa de diálogo.

4. Clique em Avançar.

   A caixa de diálogo Credenciais do nó será aberta.

   Se os nomes de usuário e as senhas fornecidos estiverem corretos, uma marca de seleção verde será mostrada no campo Verificado. Se os nomes de usuário e as senhas fornecidos não estiverem corretos, um ponto de exclamação vermelho será mostrado no campo Verificado.

5. Siga um destes procedimentos:

   - Para adicionar os nós, verifique se todos os nomes de usuário e senhas estão corretos. Para alterar as credenciais de um determinado nó, clique no campo Nome do nó.

     A caixa de diálogo Validar credenciais é aberta.

     Preencha os campos obrigatórios da caixa de diálogo Validar credenciais e clique em OK.

   - Para aplicar um nome de usuário e senha globais a todos os nós, preencha os campos Nome de usuário e Senha e clique em Aplicar à seleção de.

     O nome de usuário e a senha globais são aplicados a todos os nós.

   Clique em Concluir.

Os nós são adicionados.

Adicionar nós de servidores CA ARCserve Central Host-Based VM Backup

O CA ARCserve Central Host-Based VM Backup é um aplicativo que permite fazer o backup de máquinas virtuais por meio de uma instância do CA ARCserve D2D instalada em um servidor proxy de backup. O CA ARCserve Central Virtual Standby permite adicionar os nós que os servidores do CA ARCserve Central Host-Based VM Backup estão protegendo, de modo que seja possível criar instantâneos do ponto de recuperação para os nós. As máquinas virtuais devem ter as diretivas do CA ARCserve D2D atribuídas, e as diretivas devem ter sido atribuídas usando o CA ARCserve Central Host-Based VM Backup.

Esteja ciente do seguinte:

- O CA ARCserve Central Virtual Standby permite usar vários métodos para adicionar nós:
  - Adicionar nós manualmente
  - Adicionar nós de um arquivo de texto.
  - Adicionar nós de servidores CA ARCserve Central Host-Based VM Backup

  O CA ARCserve Central Virtual Standby permite aplicar políticas diretamente nos nós, ao passo que com o CA ARCserve Central Host-Based VM Backup é possível aplicar diretivas nos servidores proxy de backup. Esse comportamento continua após adicionar nós de servidores do CA ARCserve Central Host-Based VM Backup.

  Observação: para obter informações sobre a atribuição de diretivas do CA ARCserve D2D a nós de máquinas virtuais, consulte o *Guia do Usuário do CA ARCserve Central Host-Based VM Backup*.

- O Virtual Standby não pode acionar instantâneos do ponto de recuperação de nós que foram adicionados automaticamente de servidores do CA ARCserve Central Host-Based VM Backup. No entanto, é possível acionar instantâneos do ponto de recuperação de nós que foram adicionados manualmente de servidores do CA ARCserve Central Host-Based VM Backup.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, selecione Nó.

   A tela Nó é exibida.

2. Na categoria Nó, clique em Adicionar e, em seguida, clique em Adicionar a máquina virtual a partir do servidor do CA ARCserve Central Host-Based VM Backup no menu pop-up.

   A caixa de diálogo Adicione a máquina virtual a partir do servidor do CA ARCserve Central Host-Based VM Backup é aberta.

3. Preencha os campos abaixo na caixa de diálogo Adicionar VM de um servidor do CA ARCserve Central Host-Based VM Backup:

   - **Nome da máquina--**permite especificar o endereço IP ou o nome do servidor do CA ARCserve Central Host-Based VM Backup.
   - **Nome de usuário--**permite especificar o nome de usuário necessário para fazer logon no servidor do CA ARCserve Central Host-Based VM Backup.
   - **Senha--**permite especificar a senha necessária para fazer logon no servidor do CA ARCserve Central Host-Based VM Backup.
   - **Porta--**permite especificar o número de porta que você deseja que o aplicativo use para se comunicar com o servidor do CA ARCserve Central Host-Based VM Backup.
   - **Usar HTTPS -** permite especificar o uso de comunicação HTTPS segura.

   Clique em OK.

   Ocorre um dos seguintes eventos:

   - Se esta for a primeira vez que estiver importando nós deste sistema do ESX Server, o Virtual Standby importa todas as máquinas virtuais que contêm uma atribuição da diretiva do CA ARCserve Central Host-Based VM Backup. Após a conclusão do processo de importação, é possível verificar os nós na tela Nós.
   - Se não for a primeira vez, a caixa de diálogo Adicionar VM do servidor do CA ARCserve Central Host-Based VM Backup fornece uma lista dos nós que foram importados anteriormente. Uma caixa de diálogo é exibida e pergunta se deseja substituir as informações para os nós importados anteriormente.
   - Se o aplicativo não detectar novos nós, a caixa de diálogo Adicione a máquina virtual a partir do servidor do CA ARCserve Central Host-Based VM Backup é fechada. Em seguida, uma mensagem é exibida indicando que nenhum nó foi importado.

4. Execute uma das seguintes ações:

   - **Para adicionar os nós recém-detectados e substituir os detectados anteriormente:** clique na caixa de seleção ao lado dos nós detectados como já importados e, em seguida, clique em OK.

     O aplicativo adiciona os nós detectados recentemente e substitui os detectados anteriormente. O aplicativo substitui apenas o status atual e as credenciais que foram aplicadas aos nós detectados anteriormente.

   - **Para adicionar os nós recém-detectados (sem importar e substituir os nós detectados anteriormente):** não clique na caixa de seleção ao lado dos nós detectados como já importados e, em seguida, clique em OK.

O aplicativo adiciona somente os nós detectados recentemente. O aplicativo não substitui os nós detectados anteriormente.

- **Para sair sem adicionar nós detectados recentemente e nós detectados anteriormente**, clique em Cancelar.

  O aplicativo não adiciona nós.

5. (opcional) Clique em Atualizar na barra de ferramentas para verificar se todos os nós adicionados recentemente aparecem na lista de nós.

Os nós são adicionados.

Observação: quando as informações do CA ARCserve D2D são atualizadas no servidor do CA ARCserve Central Host-Based VM Backup, o servidor informa automaticamente o CA ARCserve Central Virtual Standby para importar as máquinas virtuais do CA ARCserve Central Host-Based VM Backup e reimplantar as diretivas. Se o CA ARCserve Central Virtual Standby não estiver disponível, você poderá importar as máquinas virtuais do CA ARCserve Central Host-Based VM Backup.

Atualizar nós

O Virtual Standby permite atualizar informações sobre os nós adicionados anteriormente.

Observação: não é possível atualizar nós que foram importados de um servidor do CA ARCserve Central Host-Based VM Backup.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, selecione Nó.

   A tela Nó é exibida.

2. Na barra Grupos, clique no grupo Todos os nós ou clique no nome de grupo contendo os nós que deseja atualizar.

   Os nós associados ao grupo são exibidos na lista de nós.

3. Clique nos nós que deseja atualizar e, em seguida, clique em Atualizar nó no menu pop-up.

   A caixa de diálogo Atualizar nó é exibida.

   Observação: para atualizar todos os nós no grupo de nós, clique com o botão direito do mouse no nome do grupo de nós e, em seguida, clique em Atualizar nó no menu pop-up.

4. Atualize os detalhes do nó, conforme necessário.

   Observação: para atualizar vários nós na lista de nós, selecione os nós desejados, clique com o botão direito do mouse em qualquer nó e clique em Atualizar nó no menu pop-up. O nome de usuário e a senha são os mesmo para todos os nós selecionados. Por padrão, a opção e o Especificar novas credenciais e a caixa de seleção Assumir controle do nó estão selecionados. É possível especificar um novo nome de usuário e senha para os nós selecionados e é possível forçar este servidor a administrar os nós. Além disso, é possível selecionar Usar credenciais existentes para aplicar o nome de usuário e senha atuais. Os campos são desativados.

5. Clique em OK.

   A caixa de diálogo Atualizar nó é fechada e os nós são atualizados.

   Observação: se forem feitas alterações em nós do CA ARCserve D2D, a caixa de diálogo Atualizar nó é aberta para que você possa especificar mais detalhes.

6. (Opcional) Se as informações atualizadas não forem exibidas na lista de nós, clique em Atualizar na barra de ferramentas.

O nó é atualizado.

Excluir nós

O Virtual Standby permite excluir nós do seu ambiente.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Nó na barra de navegação para abrir a tela Nó.

2. Na barra de Grupos, clique no grupo Todos os nós ou clique no nome de grupo contendo o nó que você deseja excluir.

   Os nós associados ao grupo são exibidos na lista de nós.

3. Selecione um ou mais nós que desejar excluir e, em seguida, clique em Excluir na barra de ferramentas.

   Uma mensagem de confirmação é exibida.

4. Siga um destes procedimentos:

   - Clique em Sim para excluir o nó.

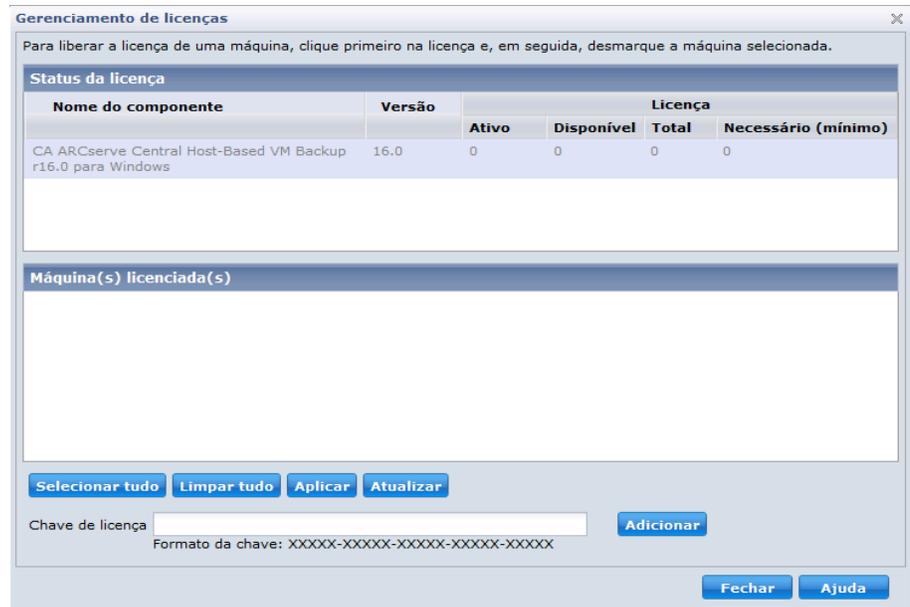
Clique em Não se não desejar excluir o nó.

Liberar licenças a partir de nós

O licenciamento do CA ARCserve Central Virtual Standby funciona em um mecanismo com base na contagem. O licenciamento com base na contagem fornece uma única licença geral para o nó, com um número predeterminado de direitos de licença ativa incluído no pool de licenças geral. Cada nó que usa a licença recebe uma licença ativa do pool, por ordem de chegada, até que o número total de direitos de licença disponível seja atingido. Se todos os direitos de licença ativa forem aplicados e você deseja adicionar uma licença a um nó diferente, libere os direitos de licença de um ou mais nós para aumentar a contagem de licenças disponível antes que outro nó possa usá-la.

Para liberar licenças a partir de nós

1. Efetue logon no aplicativo.
2. Na tela principal, abra a caixa de diálogo Gerenciamento de licenças clicando em Ajuda e em Gerenciar licenças.

   A caixa de diálogo Gerenciamento de licenças é aberta e exibe uma lista das licenças aplicadas aos computadores físicos e a máquinas virtuais do VMware e Hyper-V, conforme ilustrado na seguinte caixa de diálogo:

3. Na seção Status da licença, selecione a licença que deseja liberar dos nós.

   Os nós que usam a licença são exibidos na seção Máquinas licenciadas, na caixa de diálogo Gerenciamento de licenças.

4. Marque a caixa ao lado do nó de que deseja liberar a licença.

   Observação: clique em Desmarcar tudo para desmarcar a caixa de seleção ao lado de todos os nós exibidos na seção Máquinas licenciadas da caixa de diálogo Gerenciamento de licenças.

5. Clique em Aplicar.

   A licença e liberada do nó especificado.

6. (Opcional) Clique em Atualizar para atualizar a lista de nós que usam a licença especificada.

Interromper nós de monitoramento no servidor de monitoramento

O CA ARCserve Central Virtual Standby permite interromper os nós de monitoramento na guia Virtual Standby no servidor de monitoramento.

Importante! Ao interromper o monitoramento de nós, as máquinas no modo de espera virtual talvez não apresentem os instantâneos de ponto de recuperação mais recentes necessários para ligá-las. Além disso, é possível ligar as máquinas virtuais para os nós que o monitoramento foi interrompido (manualmente) somente a partir do sistema do hypervisor.

Para interromper nós de monitoramento no servidor de monitoramento

1. Efetue logon no servidor de monitoramento.

   Observação: para obter mais informações, consulte Efetuar logon nos servidores de monitoramento (na página 42).

2. Depois que o servidor de monitoramento for aberto, clique na guia Virtual Standby.

   A tela Virtual Standby é exibida.

3. Na árvore Origens, expanda Tudo, Origem em execução, Ação necessária ou VM em execução para localizar o nó de origem que deseja interromper o monitoramento.

4. Com o botão direito, clique no nó que deseja interromper o monitoramento e, em seguida, clique em Interromper monitoramento no menu pop-up.

   Uma mensagem de aviso será exibida.

5. Se tiver certeza de que deseja interromper o monitoramento do nó especificado, clique em Sim.

O nó é removido da árvore Origens e o servidor de monitoramento interrompe o monitoramento do nó.

Atualizar nós e diretivas depois de alterar o nome do host no servidor do CA ARCserve Central Applications

Depois de alterar o nome de host do servidor do CA ARCserve Central Virtual Standby, atualize os nós e as diretivas aplicadas aos nós. Realize essas tarefas para manter o relacionamento entre o servidor do CA ARCserve Central Virtual Standby e os nós que o servidor do CA ARCserve Central Virtual Standby está protegendo. A tabela abaixo descreve os possíveis cenários e a ação corretiva para cada cenário.

Cenário	Ação corretiva
O nó foi adicionado depois que o nome de host do servidor do CA ARCserve Central Virtual Standby foi alterado.	Nenhuma ação necessária.

Cenário	Ação corretiva
O nó foi adicionado depois que o nome de host do servidor do CA ARCserve Central Virtual Standby foi alterado e a diretiva foi aplicada ao nó.	Atualize o nó. Para obter mais informações, consulte Atualizar nós (na página 48).
O nó foi adicionado antes do nome de host do servidor do CA ARCserve Central Virtual Standby ser alterado e a diretiva ser aplicada ao nó.	Aplique a diretiva novamente. Para obter mais informações, consulte Implantar diretivas (na página 39).

Tarefas de Gerenciamento de grupo de nós

O Virtual Standby permite gerenciar os grupos de nós do CA ARCserve D2D que você está protegendo.

Esta seção contém os seguintes tópicos:

Modificar grupos de nós

O aplicativo permite modificar os grupos de nós que você criou. Você pode adicionar e remover nós de grupos de nós e alterar o nome de grupos de nós.

Observação: não é possível modificar as seguintes grupos de nós:

- **Todos os nós -** contém todos os nós associados ao aplicativo.
- **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
- **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
- **SQL Server -** contém todos os nós associados ao aplicativo e o Microsoft SQL Server está instalado.
- **Exchange -** contém todos os nós associados ao aplicativo e o Microsoft Exchange Server está instalado.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na Barra de navegação na página inicial, clique em Nó.

   A tela Nó é exibida.

2. Clique no grupo de nós que deseja modificar e, em seguida, clique em Modificar na barra de ferramentas Grupo de nós.

   A caixa de diálogo Modificar grupo é aberta.

3. Para modificar o Nome do grupo, especifique um novo nome no campo Nome do grupo.

4. Para adicionar nós ao grupo de nós, selecione um ou mais nós para adicionar ao grupo de nós e clique na seta à direita.

   Os nós passam da lista Nós disponíveis para a lista Nós selecionados e são atribuídos ao grupo de nós.

   Observação: para mover todos os nós da lista Nós disponíveis para a lista Nós selecionados, clique na seta dupla à direita.

5. Para remover nós do grupo de nós, clique na seta à esquerda ou na seta dupla à esquerda para remover um dos nós ou todos eles, respectivamente.

6. (Opcional) Para filtrar os nós disponíveis com base em critérios comuns, especifique um valor de filtragem no campo Filtragem pelo nome do nó.

   Observação: o campo Filtro permite o uso de caracteres curinga.

   Por exemplo, usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc. Para limpar os resultados do filtro, clique no X no campo Filtro.

7. Clique em OK.

O grupo de nós é modificado.

Excluir grupos de nós

O aplicativo permite excluir os Grupos de nós que você criou.

Não é possível excluir os seguintes grupos de nós:

- **Todos os nós -** contém todos os nós associados ao aplicativo.
- **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
- **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
- **SQL Server -** contém todos os nós associados ao aplicativo, e o Microsoft SQL Server está instalado nos nós.
- **Exchange -** contém todos os nós associados ao aplicativo, e o Microsoft Exchange Server está instalado nos nós.

Observação: o processo de exclusão dos grupos de nós não exclui nós individuais do aplicativo.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.

2. Clique no grupo de nós que você deseja excluir e, em seguida, clique em Excluir na barra de ferramentas do grupo de nós.

   A caixa de diálogo de Mensagem de confirmação é aberta.

3. Se tiver certeza de que deseja excluir o grupo de nós, clique em Sim.

   Observação: clique em Não se você não deseja excluir o grupo de nós.

O grupo de nós é excluído.

Filtrar grupos de nós

O Virtual Standby permite usar filtros para exibir os nós do CA ARCserve D2D em um grupo com um determinado aplicativo instalado. O Virtual Standby permite filtrar os nós que têm os seguintes aplicativos instalados:

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

Para filtrar grupos de nós

1. Efetue logon no servidor do Virtual Standby e abra o Virtual Standby.

   Na barra de navegação na página inicial, selecione Nó.

   A tela Nó é exibida.

2. Na lista de grupos, clique no grupo que deseja filtrar.

   Observação: você pode filtrar todos os grupos padrão (todos os nós, não atribuídos, SQL Server e Exchange) e todos os grupos com nomes personalizados.

   Na barra de ferramentas Filtro, clique na caixa de seleção ao lado do aplicativo que deseja filtrar.

O grupo de nós é filtrado.

Tarefas de gerenciamento de diretivas do Virtual Standby

O Virtual Standby permite gerenciar as diretivas de conversão que você usa para proteger seus nós do CA ARCserve D2D.

Esta seção contém os seguintes tópicos:

Editar ou copiar diretivas

O Virtual Standby permite editar e copiar diretivas depois de serem criadas.

Para editar diretivas

1. Efetue logon no servidor do Virtual Standby e abra o Virtual Standby.

   Na barra de navegação na página inicial, clique em Diretivas.

   A janela Diretiva é aberta.

2. Na tela Diretivas, clique na caixa de seleção ao lado de uma diretiva e execute uma das seguintes ações:

   - Clique em Editar na barra de ferramentas e edite a diretiva selecionada.
   - Clique em Copiar na barra de ferramentas para copiar e criar uma nova diretiva a partir da diretiva selecionada.

     Observação: ao copiar uma diretiva, a caixa de diálogo Copiar diretiva é aberta. Especifique um nome para o nova diretiva e clique em OK.

   A caixa de diálogo Editar diretiva é aberta.

Se desejar alterar o nome da diretiva, especifique um nome no campo Nome da diretiva.

3. Se desejar alterar o nome da diretiva, especifique um nome no campo Nome da diretiva.

4. Clique na guia Modo de espera virtual.

   As opções Servidor de virtualização, Máquina virtual e Configurações substitutas são exibidas.

5. Clique em Servidor de virtualização.

   As opções do Servidor de virtualização são exibidas.

6. Preencha as seguintes opções do servidor de virtualização:

   Sistemas VMware:

   - **Tipo de virtualização -** clique em VMware.
   - **Host do ESX/vCenter--**especifique o nome de host do sistema ESX ou vCenter Server.
   - **Nome de usuário** - especifique o nome de usuário necessário para fazer logon no sistema VMware.

     Observação: a conta especificada deve ser uma conta administrativa ou uma conta com privilégios administrativos no sistema ESX ou vCenter Server.

   - **Senha -** especifique a senha para o nome do usuário necessária para fazer logon no sistema VMware.
   - **Protocolo -** especifique HTTP ou HTTPS, dependendo do protocolo que você deseja usar para a comunicação entre o nó do CA ARCserve D2D de origem e o servidor de monitoramento.
   - **Porta -** especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o servidor de monitoramento.
   - **Nó do ESX -** os valores neste campo variam de acordo com o valor especificado no campo Host do ESX/vCenter:
     - **Sistemas ESX Server -** ao especificar um sistema ESX Server no campo Host do ESX/vCenter, esse campo exibe o nome do host do sistema ESX Server.
     - **Sistemas vCenter Server -** ao especificar um sistema vCenter Server no campo Host do ESX/vCenter, esse campo permite especificar (a partir de uma lista suspensa) o sistema ESX Server que deseja associar a tal diretiva.

- **Servidor de monitoramento** - especifique o nome do host do servidor do qual deseja obter o status do servidor de origem monitorado.

  Observação: o servidor de monitoramento pode ser qualquer computador físico ou máquina virtual desde que o servidor não esteja funcionando como o servidor proxy para uma implementação do CA ARCserve Central Host-Based VM Backup.

- **Nome de usuário** - especifique o nome de usuário necessário para fazer logon no sistema de monitoramento.
- **Senha -** especifique a senha para o nome do usuário necessária para fazer logon no servidor de monitoramento.
- **Protocolo -** especifique HTTP ou HTTPS, dependendo do protocolo que você deseja usar para a comunicação entre o servidor CA ARCserve Central Virtual Standby e o sistema do ESX Server (servidor de monitoramento).
- **Porta -** especifique a porta que você deseja usar para a transferência de dados entre o servidor CA ARCserve Central Virtual Standby e o sistema do ESX Server (servidor de monitoramento).
- **Usar o servidor de monitoramento como proxy para a transferência de dados -** especifique essa opção para permitir que o servidor de monitoramento copie os dados de conversão do nó de origem do CA ARCserve D2D para o armazenamento de dados do ESX Server. Com essa opção ativada, o Virtual Standby transfere os dados de conversão do nó de origem para o armazenamento de dados do ESX Server usando a comunicação de canal de fibra, que é mais rápido do que usar a comunicação LAN, para transferência de dados.

  Observação: a opção Usar o servidor de monitoramento como proxy para a transferência de dados fica ativada por padrão. É possível desativar essa opção para permitir que o servidor de origem do CA ARCserve D2D copie os dados de conversão diretamente para o armazenamento de dados no sistema ESX Server.

Sistemas Hyper-V:

- **Tipo de virtualização -** clique em Hyper-V.

  Observação: quando você clica em Hyper-V, as opções de monitoramento não estão acessíveis. Isso acontece porque o servidor Hyper-V assume a função do servidor de monitoramento.

- **Nome do Host Hyper-V** - especifique o nome do host do sistema Hyper-V.
- **Nome de usuário** - especifique o nome de usuário necessário para fazer logon no sistema Hyper-V.

  Observação: a conta especificada deve ser uma conta administrativa ou uma conta com privilégios administrativos no sistema Hyper-V.

- **Senha -** especifique a senha para o nome do usuário necessária para fazer logon no sistema Hyper-V.
- **Porta -** especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o servidor de monitoramento.
- **Servidor de monitoramento** - especifique o nome do host do servidor do qual deseja obter o status do servidor de origem monitorado.
- **Nome de usuário** - especifique o nome de usuário necessário para fazer logon no sistema de monitoramento.
- **Senha -** especifique a senha para o nome do usuário necessária para fazer logon no servidor de monitoramento.
- **Protocolo -** especifique HTTP ou HTTPS, dependendo do protocolo que você deseja usar para a comunicação entre o servidor CA ARCserve Central Virtual Standby e o sistema do Hyper-V Server (servidor de monitoramento).
- **Porta -** especifique a porta que você deseja usar para a transferência de dados entre o servidor CA ARCserve Central Virtual Standby e o sistema do Hyper-V Server (servidor de monitoramento).

Clique em Máquina virtual.

As opções de máquina virtual são exibidas.

7. Preencha as seguintes opções de máquina virtual:

   Sistemas VMware:

   Aplique as opções a seguir da máquina virtual para sistemas VMware:

   - **Prefixo do nome da VM--**especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual do sistema ESX Server.

     Valor padrão: CAVM_

   - **Pool de recursos da VM -** especifique o nome do pool de recursos no qual a máquina virtual em modo de espera será agrupada.

   - **Contagem de CPU -** especifique a contagem de CPU mínima e máxima suportada pela máquina virtual em modo de espera.

   - **Memória -** especifique a quantidade total de RAM (em MB) a ser alocada para a máquina virtual em modo de espera.

     Observação: a quantidade de RAM especificada deve ser um múltiplo de dois.

   - **Armazenamento de dados da VM -** especifique o local onde deseja armazenar os dados de conversão.

     - **Especificar um armazenamento de dados para todos os discos virtuais -** permite que o aplicativo copie todos os discos relacionados à máquina virtual para um armazenamento de dados.

     - **Especificar um armazenamento de dados para cada disco virtual -** permite que o aplicativo copie informações relacionadas ao disco da máquina virtual para o armazenamento de dados correspondente.

   - **Redes da VM -** permite definir NICs, redes virtuais e os caminhos que o sistema ESX Server usa para se comunicar com as máquinas virtuais.

     - **Especificar um tipo de adaptador de rede para cada NIC e conectar o adaptador de rede à seguinte rede virtual -** permite definir como mapear o NIC virtual à rede virtual. Especifique essa opção quando a máquina virtual contiver NICs virtuais e uma rede virtual.

     - **Especificar um tipo de adaptador de rede e uma rede virtual para cada NIC -** permite definir o nome da rede virtual que deseja que o NIC use para se comunicar.

Sistemas Hyper-V:

Aplique as opções a seguir da máquina virtual para sistemas Hyper-V:

- **Configurações básicas da VM -** conclua as seguintes configurações básicas:
  - **Prefixo do nome da VM -** especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual do sistema Hyper-V.

    Valor padrão: CAVM_

    Contagem de CPU - especifique a contagem de CPU mínima e máxima suportada pelo sistema virtual no modo de espera.
  - **Memória -** especifique a quantidade total de RAM (em MB) a ser alocada para a máquina virtual em modo de espera.

    Observação: a quantidade de RAM especificada deve ser um múltiplo de quatro.
- **Caminho da VM -** especifique uma das seguintes opções de caminho de VM:
  - **Especificar um caminho para todos os discos virtuais -** especifique o local no servidor Hyper-V onde deseja armazenar os dados de conversão.
  - **Especificar um caminho para cada disco virtual -** especifique o local no servidor Hyper-V onde deseja armazenar os dados de conversão para cada disco virtual.

  Observação: o CA ARCserve Central Virtual Standby não oferece suporte à criação de imagens de disco virtual (arquivos VHD) em volumes compactados e volumes que foram criptografados pelo sistema de arquivos. Se o caminho especificado residir em volumes compactados ou criptografados do Hyper-V, o Virtual Standby impede a criação da diretiva.
- **Rede da VM -** permite definir NICs, redes virtuais e os caminhos que o sistema Hyper-V Server usa para se comunicar com as máquinas virtuais. Especifique uma das seguintes opções e preencha os campos solicitados.
  - **Especificar um tipo de adaptador de rede para cada NIC e conectar o adaptador de rede à seguinte rede -** permite definir como mapear a NIC virtual para a rede virtual. Especifique essa opção quando a máquina virtual contiver NICs virtuais e uma rede virtual.
  - **Especificar um tipo de adaptador de rede e uma rede virtual para cada NIC -** permite definir o nome da rede virtual que deseja que o NIC use para se comunicar.

Clique em Configurações substitutas.

As opções de Configurações substitutas são exibidas.

8. Preencha as seguintes opções de Configurações substitutas:

   Recuperação:

   Selecione um dos seguintes métodos:

   - **Iniciar a máquina virtual manualmente -** permite ligar e configurar manualmente máquinas virtuais quando o servidor de origem falha ou interrompe a comunicação. Especifique esta opção quando preferir analisar a causa da falha antes de configurar as máquinas virtuais e permitir aos servidores funcionarem como servidores de origem.
   - **Iniciar a máquina virtual automaticamente -** permite ligar e configurar automaticamente máquinas virtuais quando o servidor de origem falha ou interrompe a comunicação. Especifique esta opção quando deseja permitir que as máquinas virtuais parem de funcionar como servidores de origem imediatamente após os servidores de origem falharem ou interromperem a comunicação.

   Observação: a opção de recuperação padrão é Iniciar manualmente a máquina virtual.

   Propriedades do sinal de monitoramento:

   - **Tempo limite--**especifique o tempo que o servidor de monitoramento deve aguardar um sinal de monitoramento antes de ligar o instantâneo de um ponto de recuperação.
   - **Frequência--**especifique a frequência com que o servidor de origem fará a comunicação dos sinais de monitoramento com o servidor do monitor.

     Exemplo: o valor de tempo limite especificado é 60. O valor de frequência especificado é 10. O servidor de origem comunicará sinais de monitoramento em intervalos de 10 segundos. Se o servidor de monitoramento não detectar um sinal de monitoramento em 60 segundos do último sinal detectado, ele ligará a máquina virtual usando o instantâneo do ponto de recuperação mais recente.

   Clique na guia Preferências.

   A janela de opções de Alertas por emails é exibida.

9. Preencha as seguintes opções de Alertas por email:
   - **Sinal de monitoramento faltando para a máquina de origem -** o Virtual Standby envia notificações de alerta quando o servidor de monitoramento não detecta um sinal de monitoramento no servidor de origem.
   - **VM ligada para a máquina de origem configurada para ser ligada automaticamente -** o Virtual Standby envia notificações de alerta quando ele liga uma máquina virtual que foi configurada para ligar automaticamente quando um sinal de monitoramento não é detectado.
   - **Sinais de monitoramento ausentes para a máquina de origem configurada para ser ligada manualmente -** o Virtual Standby envia notificações de alerta quando ele não detecta um sinal de monitoramento de um servidor de origem que não esteja configurado para ligar automaticamente.
   - **Espaço livre de armazenamento da VM abaixo de -** o Virtual Standby envia notificações de alerta quando detecta espaço livre em disco insuficiente no caminho definido pelo HyperVisor. A detecção ocorre quando a quantidade de espaço livre em disco é menor do que o limite definido pelo usuário. O limite máximo pode ser representado como um valor absoluto (em MB) ou uma porcentagem da capacidade do volume.
   - **Erros/falhas/paralisação no Virtual Standby -** o Virtual Standby envia notificações de alerta quando detecta um erro que ocorreu durante o processo de conversão.
   - **Operação do Virtual Standby realizada com êxito -** o Virtual Standby envia notificações de alerta quando detecta que uma máquina virtual foi ligada com êxito.
   - **O Hypervisor não está acessível -** o Virtual Standby envia notificações de alerta quando detecta que ele não pode se comunicar com o sistema ESX Server ou com o sistema Hyper-V.
   - **Falha na licença -** especifica que o Virtual Standby deve enviar notificações de alerta quando detectar problemas de licenciamento em servidores do Virtual Standby, servidores de origem e servidores de monitoramento.
   - **O Virtual Standby não foi iniciado com êxito a partir do instantâneo do ponto de recuperação -** o Virtual Standby envia notificações de alerta quando detecta que uma máquina virtual não foi ligada automaticamente e a opção de início automático da recuperação de substituição da máquina virtual é especificada.

   Clique em Salvar.

A diretiva é editada.

Remover atribuição de nós de diretivas

O Virtual Standby permite que você remova a atribuição de nós de diretivas. O Virtual Standby não permite atribuir várias diretivas para nós. Se deseja atribuir nós a novas diretivas, deve-se primeiro remover a atribuição da diretiva atual dos nós antes de poder atribuir uma nova diretiva aos nós.

Siga estas etapas:

1. Efetue logon no servidor do Virtual Standby e abra o Virtual Standby.

   Na barra de navegação na página inicial, clique em Diretivas para abrir a tela Diretivas.

2. Na lista de diretivas, clique na diretiva da qual deseja remover a atribuição de nós.

   Informações detalhadas sobre a diretiva especificada são exibidas na guia Detalhes de diretiva e na guia Atribuição de diretiva.

3. Clique na guia Detalhes da diretiva para exibir informações detalhadas sobre a diretiva.

   (Opcional) Clique em Editar na barra de ferramentas de Diretivas para editar as configurações atuais da diretiva.

   Observação: para obter mais informações, consulte Editar diretivas (na página 56).

4. Clique na guia Atribuição de diretiva.

   Clique em Atribuir e remover a atribuição na guia Atribuição de diretivas para abrir a caixa de diálogo Atribuir/Remover a atribuição de diretivas.

5. Especifique os seguintes campos da caixa de diálogo Atribuir/Remover a atribuição de diretivas:

   - **Grupo--**selecione o nome do grupo que contém a diretiva que deseja atribuir.
   - **Filtro Nome do nó--**permite filtrar os nós disponíveis com base em critérios comuns.

   Observação: o campo Filtro permite o uso de caracteres curinga.

   Exemplos:

   - Usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc.
   - Usar *.123 permite filtrar todos os nós que contenham .123 no endereço IP.

   Observação: para limpar os resultados do filtro, clique no x no campo Filtro.

6. Execute uma das seguintes ações:
   - **Remover a atribuição de um nó--**na lista de nós selecionados, localize o nó cuja atribuição deseja remover da diretiva.

     Clique na seta única à esquerda.

     O nó é movido da lista de nós selecionados para a lista de nós disponíveis.
   - **Remover a atribuição de nós--**na lista de nós selecionados, clique na seta dupla à esquerda.

     Todos os nós são movidos da lista de nós selecionados para a lista de nós disponíveis.

   Clique em OK.

A atribuição dos nós é removida da diretiva.

Excluir diretivas

O Virtual Standby permite excluir diretivas criadas anteriormente.

Observação: o Virtual Standby não permite que você exclua as diretivas que são atribuídas a nós. Para excluir diretivas que contêm nós atribuídos, você deve primeiro remover a atribuição de nós da diretiva para depois excluí-la. Para obter informações sobre como remover a atribuição de nós de uma diretiva, consulte Remover atribuição de nós de diretivas (na página 64).

Para excluir diretivas

1. Efetue logon no servidor do Virtual Standby e abra o Virtual Standby.

   Na barra de navegação na página inicial, clique em Diretivas do VCM.

   A janela Diretiva é aberta.
2. Na lista de diretivas, clique na diretiva que deseja excluir.
3. Clique em Excluir na barra de ferramentas de Diretivas.

   Uma mensagem de confirmação de exclusão é exibida.
4. Clique em Sim para excluir a diretiva.

   Observação: se você excluir uma diretiva por engano, será necessário recriá-la. Se você não deseja excluir a diretiva, clique em Não.

A diretiva é excluída.

Tarefas de Configuração de aplicativo

O Virtual Standby permite especificar configurações de alertas de email e como deseja atualizar sua instalação.

Esta seção contém os seguintes tópicos:

Definir as configurações de email

É possível especificar configurações de email para uso com seu aplicativo, de modo a enviar automaticamente alertas sob as condições determinadas.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Configuração para abrir a tela Configuração.

2. No painel Configuração, clique em Configuração de email para exibir as opções de Configuração de email.

3. Preencha os seguintes campos:
   - **Serviço** - especifique o tipo de serviço de email na lista suspensa. (Google Mail, Yahoo Mail, Live Mail ou Outro).
   - **Servidor de email**--especifique o nome do host do servidor SMTP que o CA ARCserve Central Applications deve usar para enviar email.
   - **Requer autenticação**-selecione essa opção quando o servidor de email especificado exigir autenticação. O nome da conta e a senha serão necessários.
   - **Assunto**--especifique um assunto de email padrão.
   - **De**--especifique o endereço de email para o qual o email está sendo enviado.
   - **Destinatário**--especifique um ou mais endereços de email, separados por um ponto e vírgula (;), para os quais o email será enviado.
   - **Usar SSL** - selecione essa opção se o servidor de email especificado exigir uma conexão segura (SSL).
   - **Enviar STARTTLS** - selecione essa opção se o servidor de email especificado exigir o comando STARTTLS.
   - **Usar formato HTML** - permite enviar mensagens de email no formato HTML. (selecionado por padrão)
   - **Ativar configurações de proxy** - selecione essa opção se houver um servidor proxy. Em seguida, especifique as configurações do servidor proxy.
4. Clique em Testar email para verificar se as definições das configurações de email estão corretas.
5. Clique em Salvar.

   Observação: pode-se clicar em Redefinir para reverter aos valores salvos anteriormente.

A configuração de email é aplicada.

Configurar atualizações automáticas

O CA ARCserve Central Virtual Standby permite definir quando verificar atualizações do produto e a frequência com que a instalação do Virtual Standby deve ser atualizada.

Para configurar atualizações automáticas

1. Efetue logon no aplicativo.
2. Clique em Configuração na barra de navegação para abrir a tela Configuração.
3. No painel Configuração, clique em Atualizar configuração.

   As opções de configuração de atualização são exibidas.

4. Selecione um servidor de download.
   - **CA Server** - clique em Configurações de proxy para as seguintes opções:
     - **Usar configurações de proxy do navegador -** permite usar as credenciais fornecidas para as configurações de proxy do navegador.

       Observação: a opção Usar configurações de proxy do navegador afeta o Internet Explorer e o Chrome.
     - **Configurar definições de proxy** - especifique o Endereço IP ou o Nome do host do servidor proxy e o número de porta. Se o servidor especificado exigir autenticação, clique em O servidor proxy exige autenticação e forneça as credenciais.

       Clique em OK para voltar à Atualizar configuração.
   - **Servidor de armazenamento temporário -** se você selecionar essa opção, clique em Adicionar Servidor para adicionar um servidor de armazenamento temporário na lista. Digite o nome de host e o número da porta e clique em OK.

     Se forem especificados vários servidores de armazenamento temporário, o aplicativo tentará usar o primeiro servidor da lista. Se a conexão for bem-sucedida, os demais servidores relacionados não são usados para armazenamento temporário.
5. (Opcional) Clique em Testar conexão para verificar a conexão de servidor e aguarde até que o teste seja concluído.
6. (Opcional) Clique em Verificar atualizações automaticamente e especifique o dia e a hora. Você pode especificar uma programação diária ou semanal.

Clique em Salvar para aplicar a configuração atualizada.

Definir configurações de proxy

O CA ARCserve Central Applications permite especificar um servidor proxy para se comunicar com o suporte da CA a fim de verificar e fazer download das atualizações disponíveis. Para ativar este recurso, é necessário especificar o servidor proxy que deseja que se comunique em nome do servidor do CA ARCserve Central Applications.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Configuração na barra de navegação.

   A opção Configuração é exibida.
2. Clique em Atualizar configuração.

   As opções de configuração de atualização são exibidas.
3. Clique em Configurações de proxy.

   A caixa de diálogo Configurações de proxy é aberta.

4. Clique em uma das seguintes opções:

   - **Usar configurações de proxy do navegador --**permite que o aplicativo detecte e use as mesmas configurações de proxy que são aplicadas para o navegador para se conectar ao servidor da CA Technologies para atualizar as informações.

     Observação: esse comportamento se aplica somente aos navegadores Internet Explorer e Chrome.

   - **Definir configurações de proxy**--permite definir um servidor alternativo que o aplicativo usará para se comunicar com o suporte da CA para verificar se há atualizações. O servidor alternativo (proxy) pode ajudar a garantir a segurança, melhorar o desempenho e garantir o controle administrativo.

     Preencha os seguintes campos:

     – **Servidor proxy--** especifique o nome do host ou o endereço IP do servidor proxy.

     – **Porta--**especifique o número de porta que o servidor proxy usará para se comunicar com o site de suporte da CA.

     – **(Opcional) o servidor proxy requer autenticação--** se as credenciais de logon do servidor proxy não forem as mesmas do CA ARCserve Central Applications, clique na caixa de seleção próxima ao Servidor proxy requer autenticação, e especifique o nome de usuário e a senha necessárias para efetuar logon no servidor proxy.

       Observação: use o seguinte formato para especificar o nome de usuário: <nome de domínio>/<nome de usuário>.

   Clique em OK.

As configurações de proxy são definidas

Configurando preferências de redes sociais

O CA ARCserve Central Applications permite gerenciar as ferramentas de rede social para ajudá-lo a gerenciar o aplicativo. Você pode gerar novos feeds, especificar links para sites de redes sociais populares e selecionar sites de fonte de vídeos.

Para configurar preferências de redes sociais

1. Efetue logon no aplicativo.

   Na Barra de navegação na página inicial, clique em Configuração.

   A tela Configuração é exibida.

2. No painel Configuração, clique em Configuração de preferências.

   A opção Preferências é exibida.

3. Especifique as opções necessárias:

   - **Feed de notícias -** permite que o aplicativo exiba feeds RSS de notícias relacionadas ao CA ARCserve Central Applications e ao CA ARCserve D2D e informações do produto (do Expert Advice Center). Os feeds são exibidos na página inicial.
   - **Rede social -** permite que o aplicativo exiba ícones na página inicial para acesso ao Twitter e ao Facebook para sites de redes sociais relacionados ao CA ARCserve Central Applications e ao CA ARCserve D2D .
   - **Vídeos -** permite selecionar o tipo de vídeo para exibição dos produtos do CA ARCserve Central Applications e CA ARCserve D2D. (A opção padrão é Usar vídeos do YouTube.)

   Clique em Salvar.

   As opções de Rede social são aplicadas

4. Na barra de navegação, clique em Página Inicial.

   A Página inicial é exibida.

5. Atualize a janela do navegador.

   As opções de Rede social são aplicadas.

Modificar a conta do administrador

O CA ARCserve Central Applications permite modificar o nome de usuário, senha, ou ambos da conta do administrador depois de instalar o aplicativo. Esta conta de administrador somente é usada para exibição do nome de usuário padrão na tela de logon.

Observação: o nome de usuário especificado deve ser uma conta administrativa do Windows ou uma conta que tenha privilégios administrativos do Windows.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Configuração na barra de navegação.

   A opção Configuração é exibida.

2. Clique em Conta de administrador

3. A configuração da conta do administrador é exibida.

4. Atualize os seguintes campos, conforme necessário:

   - Nome de usuário
   - Senha

   Clique em Salvar

A conta do administrador é modificada.

Exibir logs

O Log de exibição contém informações abrangentes sobre todas as operações executadas pelo aplicativo. O log fornece uma trilha de auditoria de todas as tarefas executadas (com as atividades mais recentes listadas primeiro) e pode ser útil para a solução dos problemas que podem ocorrer.

Para exibir os logs

1. Na página inicial, clique em Exibir logs na barra de navegação.

   A tela Exibir logs é exibida.

2. Nas listas suspensas, especifique as informações de log que você deseja exibir.

   - **Gravidade:** permite especificar a gravidade do log que você deseja exibir. É possível especificar as seguintes opções de gravidade:
     - **Todos -** permite exibir todos os logs, independentemente da gravidade.
     - **Informações -** permite exibir apenas os logs que descrevem informações gerais.
     - **Erros -** permite exibir apenas os logs que descrevem erros graves que ocorreram.
     - **Avisos -** permite exibir apenas os logs que descrevem avisos de erros que ocorreram.
     - **Erros e avisos -** permite exibir apenas erros graves e aviso de erros que ocorreram.
   - **Módulo -** permite especificar o módulo para o qual você deseja exibir logs. É possível especificar as seguintes opções de módulo:
     - **Todos -** permite exibir logs sobre todos os componentes do aplicativo.
     - **Comum -** permite exibir logs sobre processos comuns.
     - **Importar nós do arquivo -** permite exibir apenas os logs sobre o processo de importação de nós do CA ARCserve D2D para o aplicativo de um arquivo.
     - **Gerenciamento de diretivas -** permite exibir apenas os logs sobre gerenciamento de diretivas.
     - **Atualizações** - permite exibir apenas os logs sobre a atualização do aplicativo.
   - **Nome do nó-** permite exibir apenas os logs de um determinado nó.

     Observação: esse campo suporta os caracteres curinga '*' e '?'. Por exemplo, digite 'lod*' para retornar todos os logs de atividades para o nome de computador iniciado por 'lod'.

Observação: as opções de Gravidade, Módulo e Nome do nó podem ser aplicadas em grupo. Por exemplo, você pode exibir erros (Gravidade) que estão relacionados a atualizações (Módulo) para o nó X (Nome do nó).

Clique em Atualizar.

Os logs são exibidos com base nas opções de exibição especificadas.

Observação: a hora exibida no arquivo de log é baseada no fuso horário do servidor de banco de dados do aplicativo.

Adicionar links à barra de navegação

Cada CA ARCserve Central Applications possui um link Adicionar nova guia na barra de navegação. Use este recurso para adicionar entradas na barra de navegação para outros aplicativos da web que deseja gerenciar. No entanto, para cada aplicativo instalado, um novo link é automaticamente adicionado à barra de navegação. Por exemplo, se você tiver instalado o CA ARCserve Central Reporting e o CA ARCserve Central Virtual Standby no "computador A" e, em seguida, iniciar o CA ARCserve Central Reporting, o CA ARCserve Central Virtual Standby é automaticamente adicionado à barra de navegação.

Observação: cada aplicativo instalado é detectado somente se outros CA ARCserve Central Applications estiverem no mesmo computador.

Siga estas etapas:

1. Na barra de navegação do aplicativo, clique no link Adicionar nova guia.
2. Especifique o nome e o URL do aplicativo ou site que deseja adicionar. Por exemplo, www.google.com.

   Como opção, é possível especificar o local de um ícone.
3. Clique em OK.

   A nova guia é adicionada à parte inferior da barra de navegação.

Lembre-se das seguintes considerações:

- Para sua conveniência, o link do Suporte da CA é adicionado por padrão.

  É possível remover a nova guia, destacando a guia e clicando no link Remover.

Página inicial do Virtual Standby

A guia Modo de espera virtual no servidor de monitoramento permite exibir informações sobre todos os servidores do CA ARCserve D2D que você está protegendo. No entanto, esta guia em servidores de origem permite exibir apenas as informações sobre o servidor de origem específico que você efetuar logon.

Esta seção contém os seguintes tópicos:

Como usar a tela Resumo do modo de espera virtual

A tela Resumo do modo de espera virtual exibe ícones que fornecem uma rápida indicação visual do status atual, juntamente com a orientação para a urgência de quaisquer ações que possam ser necessárias.

As seguintes opções são exibidas na página inicial:

Com êxito
(Nenhuma ação é necessária)

Atenção
(Uma ação será necessária em breve)

Aviso
(Ação imediata é necessária)

A tela Resumo do Virtual Standby exibe as seguintes informações:

- **Lista de servidores -** exibe uma lista de servidores de origem que este servidor de monitoramento está protegendo. A lista classifica os servidores pelo seu status atual. Por exemplo: Todos, Ação necessária, Servidor em execução e assim por diante.

  Observação: a lista de servidores é exibida apenas quando você está conectado ao servidor de monitoramento. Para obter mais informações, consulte Como usar a lista de servidores (na página 75).

- **Resumo do modo de espera virtual--**exibe informações de resumo do servidor de origem selecionado. Para obter mais informações, consulte Monitorar o status de trabalhos de conversão virtual (na página 77).

- **Configurações do modo de espera virtual--**exibe informações resumidas sobre as configurações de conversão virtual do servidor de origem selecionado. Para obter mais informações, consulte Exibir Configurações do modo de espera virtual para servidores de origem (na página 78).
- **Instantâneos do ponto de recuperação -** exibe uma lista de instantâneos de ponto de recuperação que estão disponíveis para o servidor de origem selecionado. Para obter mais informações, consulte Exibir a lista de instantâneos de ponto de recuperação (na página 78).
- **Tarefas -** exibe uma lista de tarefas que você pode executar para o servidor de origem selecionado. Para obter mais informações, consulte Tarefas de monitoramento no modo de espera virtual (na página 79).
- **Suporte e acesso público -** fornece um mecanismo que permite que você inicie várias funções relacionadas a suporte.

  Observação: para obter mais informações sobre o Suporte e acesso público, consulte a documentação do CA ARCserve D2D.

Como usar a Lista Servidores

A lista Servidores na tela Resumo do modo de espera virtual exibe uma lista de servidores de origem que estão sendo protegidos por um servidor de monitoramento. A lista classifica os servidores pelo seu status atual. Por exemplo: Todos, Ação necessária, Origem em execução e assim por diante.

Para executar tarefas de manutenção ou para exibir informações sobre o nó do CA ARCserve D2D, clique na guia Modo de espera virtual e, em seguida, clique no servidor conforme ilustrado na tela a seguir:

Exibir informações resumidas sobre a tarefa mais recente do Virtual Standby

A tela Nó permite exibir informações resumidas sobre a tarefa mais recente do Virtual Standby (conversão) de um nó. Você pode exibir informações sobre as tarefas do Virtual Standby que foram concluídas com êxito e sem êxito.

Siga estas etapas:

1. Efetue logon no servidor do Virtual Standby.

   Clique em Nós na barra de navegação para abrir a tela Nós.

2. Na coluna Status, passe o ponteiro do mouse sobre um dos ícones exibidos a seguir:

   Bem-sucedido

   Aviso

   Erro/Falha

   A caixa de mensagem Resumo de status do nó é exibida e fornece os seguintes resultados da tarefa mais recente com êxito do Virtual Standby:

   Virtual Standby mais recente

   A data e hora da tarefa do Virtual Standby mais recente que foi concluída com êxito ou sem êxito.

   Instantâneos do ponto de recuperação

   Exibe o número de pontos de recuperação que são convertidos para o nó como o Virtual Standby mais recente.

   Status do destino

   Exibe a quantidade de espaço em disco livre disponível no destino do Virtual Standby. O destino pode consistir no seguinte:

   - Um armazenamento de dados do ESX Server que é usado para converter para um sistema ESX Server.
   - Libere espaço em disco no volume onde um servidor Hyper-V armazena os instantâneos do ponto de recuperação.

3. Afaste o ponteiro do mouse do ícone de status para fechar a caixa de mensagem Resumo de status do nó.

4. É possível exibir mais informações sobre a tarefa do Virtual Standby mais recente com êxito ou sem êxito nos seguintes campos:

   Resultados da última conversão

   Resultados da tarefa do Virtual Standby mais recente que foi concluída com êxito ou sem êxito. Por exemplo, Concluído, Cancelado, Com falha.

   Hora da última conversão

   A data e hora em que a tarefa do Virtual Standby mais recente com êxito ou sem êxito foi concluída.

Monitorar o status dos trabalhos de conversão virtual

O Virtual Standby permite monitorar o status de trabalhos de conversão virtuais em andamento. Além disso, ele permite exibir informações resumidas sobre os dados de conversão virtual e as máquinas virtuais que estão protegendo os servidores de origem do seu CA ARCserve D2D.

Para monitorar o status das tarefas de conversão virtual

1. Abra a opção Modo de espera virtual e clique em Nós na barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   O CA ARCserve D2D é aberto.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

4. Clique na guia Modo de espera virtual.

   (Opcional) Se o servidor do CA ARCserve D2D é um servidor de monitoramento, clique na lista de servidores, expanda Todos, Origem em execução ou Ação necessária, e clique no servidor que você deseja monitorar.

   O Virtual Standby exibe informações sobre trabalhos de conversão virtual em andamento e informações resumidas sobre os trabalhos de conversão virtual e a máquina virtual que está protegendo o servidor.

Exibir Configurações do modo de espera virtual para servidores de origem

A tela Resumo do modo de espera virtual exibe informações sobre as máquinas virtuais que estão protegendo os servidores de origem.

Exibir a lista de Instantâneos do ponto de recuperação

A tela Modo de espera virtual exibe uma lista dos instantâneos do ponto de recuperação mais recentes.

A caixa de listagem exibe a data e a hora em que o backup do servidor do CA ARCserve D2D foi concluído.

É possível ligar máquinas virtuais da partir da lista de instantâneos do ponto de recuperação. Para obter mais informações, consulte Ligar Instantâneos do ponto de recuperação (na página 85).

Observação: se o destino de Modo de espera virtual for um servidor do VMware ESX, o número máximo de instantâneos do ponto de recuperação exibidos será 29. Se o destino de Modo de espera virtual for um servidor do Microsoft Hyper-V ESX, o número máximo de instantâneos do ponto de recuperação exibidos será 24.

Tarefas de monitoramento do CA ARCserve Central Virtual Standby

O Virtual Standby permite executar as seguintes tarefas de monitoramento:

- Pausar e continuar sinais de monitoramento (na página 79).
- Pausar e continuar as tarefas do Virtual Standby (na página 83).
- Exibir dados do log de atividades sobre conversões virtuais e instantâneos do ponto de recuperação (na página 89).
- Ligar instantâneos do ponto de recuperação (na página 85).

Pausar e retomar sinais de monitoramento no servidor do Virtual Standby

O Virtual Standby permite pausar e retomar sinais de monitoramento detectados pelo servidor de monitoramento. O sinal de monitoramento é o processo em que o servidor de origem e o servidor de monitoramento se comunicam sobre a integridade do servidor de origem. Se o servidor de monitoramento não detectar um sinal de monitoramento após um determinado período de espera, o Virtual Standby configura a máquina virtual para funcionar como o nó de origem.

Exemplos: quando pausar ou retomar sinais de monitoramento

Os exemplos a seguir descrevem quando pausar e retomar sinais de monitoramento:

- Pause o sinal de monitoramento quando desejar desativar um nó (servidor de origem) para manutenção.
- Retome o sinal de monitoramento após a conclusão das tarefas de manutenção e quando o nó (servidor de origem) estiver online.

Esteja ciente do seguinte:

- Você pode pausar e retomar os sinais de monitoramento no nível de grupo ou no nível de nó individual.
- Você pode pausar e retomar os sinais de monitoramento para um ou mais nós em uma única etapa.
- O CA ARCserve Central Virtual Standby não liga instantâneos de pontos de recuperação enquanto o sinal de monitoramento estiver em pausa.
- Ao atualizar as instalações do CA ARCserve D2D em nós de origem, o CA ARCserve Central Virtual Standby pausa o sinal de monitoramento dos nós. Para garantir que os servidores de monitoramento monitorem os nós atualizados, retome o sinal de monitoramento dos nós após concluir a atualização nos nós.

Observação: como alternativa, é possível pausar ou retomar sinais de monitoramento na tela Resumo do Virtual Standby no nó. Para obter mais informações, consulte o tópico Pausar e retomar sinais de monitoramento dos nós (na página 82).

Siga estas etapas:

1. Efetue logon no servidor do Virtual Standby.

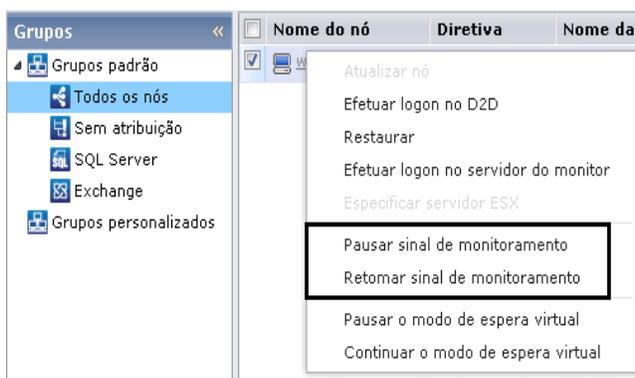
   Clique em Nós na barra de navegação para abrir a tela Nós.

2. Execute uma das seguintes ações para especificar os nós que deseja pausar ou retomar:

   - **Nível de nó**: clique no grupo que contém os nós que desejar pausar ou retomar e, em seguida, clique na caixa de seleção ao lado dos nós que desejar pausar ou retomar.
   - **Nível de grupo**: clique no grupo que contém os nós que desejar pausar ou retomar.

3. Em seguida, execute uma das seguintes ações para pausar ou retomar os sinais de monitoramento:

   - Clique em Sinal de monitoramento na barra de ferramentas e clique em Pausar ou Retomar no menu pop-up, conforme ilustrado na tela a seguir:

   - Clique com o botão direito do mouse no grupo selecionado ou clique com o botão direito do mouse nos nós e clique em Pausar sinal de monitoramento ou Retomar sinal de monitoramento no menu pop-up, conforme ilustrado na tela a seguir:

Pausar e retomar sinais de monitoramento dos nós

O Virtual Standby permite pausar e retomar sinais de monitoramento detectados pelo servidor de monitoramento. O sinal de monitoramento é o processo em que o servidor de origem e o servidor de monitoramento se comunicam sobre a integridade do servidor de origem. Se o servidor de monitoramento não detectar um sinal de monitoramento após um determinado período de espera, o Virtual Standby configura a máquina virtual para funcionar como o nó de origem.

Exemplos: quando pausar ou retomar sinais de monitoramento

Os exemplos a seguir descrevem quando pausar e retomar sinais de monitoramento:

- Pause o sinal de monitoramento quando desejar desativar um nó (servidor de origem) para manutenção.
- Retome o sinal de monitoramento após a conclusão das tarefas de manutenção e quando o nó (servidor de origem) estiver online.

Observação: como alternativa, você pode pausar e retomar os sinais de monitoramento na tela Nó do servidor do Virtual Standby. Para obter mais informações, consulte o tópico Pausar e retomar sinais de monitoramento no servidor do Virtual Standby (na página 79).

Siga estas etapas:

1. Efetue logon no servidor do Virtual Standby.

   Clique em Nós na barra de navegação para abrir a tela Nós.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja pausar ou retome o sinal de monitoramento e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   O CA ARCserve D2D é aberto.

4. Clique na guia Modo de espera virtual.

   A tela Resumo do modo de espera virtual é exibida.

5. (Opcional) Se você estiver conectado a um servidor de monitoramento, expanda Todos ou Servidor em execução na lista de servidores e clique no nó cujo sinal de monitoramento deseja pausar ou continuar.

   Observação: se o sinal de monitoramento estiver em execução, Pausar sinal de monitoramento é exibido na lista de tarefas de Conversão virtual. Se o sinal de monitoramento não estiver em execução, Continuar o sinal de monitoramento é exibido na lista de tarefas de Conversão virtual.

6. Siga um destes procedimentos:

   - Se o sinal de monitoramento estiver em execução, clique em Pausar sinal de monitoramento para interrompê-lo temporariamente.

     Exemplo: você deseja colocar o servidor offline para executar tarefas de manutenção.

   - Se o sinal de monitoramento não estiver em execução (pausado), clique em Continuar o sinal de monitoramento para retomá-lo.

     Exemplo: as tarefas de manutenção foram concluídas e você deseja colocar o servidor online.

O sinal de monitoramento pausa ou continua.

Pausar e retomar tarefas do Virtual Standby no servidor do Virtual Standby

A conversão virtual é o processo em que o Virtual Standby converte pontos de recuperação do CA ARCserve D2D de nós de origem para arquivos de dados da máquina virtual, denominados instantâneos de pontos de recuperação. No caso de um servidor de origem falhar, o Virtual Standby usa os instantâneos de pontos de recuperação para ligar uma máquina virtual no nó de origem.

Como prática recomendada, permita que o processo de conversão virtual opere continuamente. No entanto, se deseja pausar o processo de conversão virtual temporariamente, pode fazê-lo no servidor do Virtual Standby. Depois de corrigir os problemas no nó de origem, você pode continuar o processo de conversão virtual.

Observação: como alternativa, você pode pausar e retomar tarefas do Virtual Standby diretamente nos nós. Para obter mais informações, consulte o tópico Pausar e retomar tarefas do Virtual Standby nos nós (na página 84).

Siga estas etapas:

1. Efetue logon no servidor do Virtual Standby.

   Clique em Nós na barra de navegação para abrir a tela Nós.

2. Execute uma das seguintes ações para especificar os nós que você deseja que pausem ou retomem as tarefas do Virtual Standby:

   - **Nível de nó**: clique no grupo que contém os nós que desejar pausar ou retomar e, em seguida, clique na caixa de seleção ao lado dos nós que desejar pausar ou retomar.

   - **Nível de grupo**: clique no grupo que contém os nós que desejar pausar ou retomar.

3. Em seguida, execute uma das seguintes ações para pausar ou retomar as tarefas do Virtual Standby:
   - Clique em Virtual Standby na barra de ferramentas e clique em Pausar ou Retomar no menu pop-up.
   - Clique no grupo selecionado ou clique nos nós e clique em Pausar o Virtual Standby ou Retomar o Virtual Standby no menu pop-up.

Pausar e retomar tarefas do Virtual Standby nos nós

A conversão virtual é o processo em que o Virtual Standby converte pontos de recuperação do CA ARCserve D2D de nós de origem para arquivos de dados da máquina virtual, denominados instantâneos de pontos de recuperação. No caso de um servidor de origem falhar, o Virtual Standby usa os instantâneos de pontos de recuperação para ligar uma máquina virtual no nó de origem.

Como prática recomendada, permita que o processo de conversão virtual opere continuamente. No entanto, se deseja pausar o processo de conversão virtual temporariamente, pode fazê-lo no servidor do Virtual Standby. Depois de corrigir os problemas no nó de origem, você pode continuar o processo de conversão virtual.

Observação: como alternativa, você pode pausar e retomar as tarefas do Virtual Standby no servidor do Virtual Standby. Para obter mais informações, consulte o tópico Pausar e retomar tarefas do Virtual Standby no servidor do Virtual Standby (na página 83).

Siga estas etapas:

1. Abra o Modo de espera virtual e clique em Nós na barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja pausar ou retome as tarefas do Virtual Standby, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   O CA ARCserve D2D é aberto.

4. Clique na guia Modo de espera virtual.

   A tela Resumo do modo de espera virtual é exibida.

5. (Opcional) Se você estiver conectado a um servidor de monitoramento, expanda Todos ou Servidor em execução na lista Servidores e clique no nó cuja tarefa em modo de espera virtual deseja pausar ou continuar.

   Se a tarefa do Virtual Standby estiver em execução, a opção Pausar o Virtual Standby será exibida na lista de tarefas do Virtual Standby. Se a tarefa do Virtual Standby não estiver em execução, a opção Retomar o Virtual Standby será exibida na lista de tarefas do Virtual Standby.

6. Siga um destes procedimentos:

   ■ Se a tarefa em modo de espera virtual estiver em execução, clique na opção Pause Virtual Standby para pausar a tarefa temporariamente.

   ■ Se a tarefa em modo de espera virtual não estiver em execução (pausada), clique na opção Resume Virtual Standby para continuar a tarefa.

A tarefa em modo de espera virtual pausa ou continua.

Ligar máquinas no modo de espera virtual a partir de instantâneos de ponto de recuperação

O Virtual Standby pode ser configurado para ligar máquinas no modo de espera virtual automaticamente a partir de instantâneos de ponto de recuperação quando o servidor de monitoramento não detectar nenhum sinal de monitoramento do servidor de origem. Como alternativa, o Virtual Standby permite ligar as máquinas no modo de espera virtual manualmente a partir de instantâneos de ponto de recuperação, caso haja uma emergência ou falha em um servidor de origem ou caso deseje colocá-lo offline para manutenção.

Observação: as etapas a seguir descrevem como ligar manualmente máquinas no modo de espera virtual a partir de instantâneos de ponto de recuperação. Para obter informações sobre como permitir que o Virtual Standby ligue os instantâneos do ponto de recuperação automaticamente, consulte o tópico Criar diretivas (na página 30).

Siga estas etapas:

1. Abra o Virtual Standby e clique em Nós na barra de navegação para abrir a tela Nós.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados ao grupo especificado.

3. Procure e clique no nó que deseja ligar a partir de um Instantâneo do ponto de recuperação e clique em Máquina virtual no modo de espera na barra de ferramentas Ações.

   A caixa de diálogo Instantâneo do ponto de recuperação é exibida.

4. Na caixa de diálogo Instantâneo do ponto de recuperação, especifique um intervalo de data e hora para localizar o instantâneo do ponto de recuperação que deseja usar.

   Clique em Ligar VM.

A máquina virtual é ligada usando os dados contidos no instantâneo do ponto de recuperação.

Observação: após ligar a máquina virtual, poderá ser solicitado que você reinicie o computador uma ou mais vezes. Este comportamento ocorre pois o VMware instala o VMware Tools na máquina virtual e o Windows Hyper-V instala os serviços de integração.

Depois que você ligar as máquinas virtuais no Virtual Standby a partir dos instantâneos do ponto de recuperação, talvez seja preciso concluir as seguintes tarefas:

- Ativar o sistema operacional do Windows em execução na máquina virtual.
- Iniciar os backups do CA ARCserve D2D na máquina virtual.

  Observação: para obter informações sobre como criar e atribuir as diretivas de backup do CA ARCserve D2D usando o Gerenciador do CA ARCserve Central Protection, consulte o *Guia do Usuário do Gerenciador do CA ARCserve Central Protection*.

- Atualize o CA ARCserve Central Virtual Standby com o nome do host, endereço IP e as credenciais de logon na máquina virtual.
- Atribua o nó à diretiva.

  Observação: esta tarefa é necessária somente se você deseja criar instantâneos do ponto de recuperação para a máquina virtual que foi ligada. Para obter mais informações, consulte Atribuir nós a diretivas (na página 38).

Ligar máquinas no modo de espera virtual a partir do Hyper-V Manager

Se desejar ligar manualmente máquinas virtuais no Modo de espera virtual, a prática recomendada é ligar as máquinas virtuais pela tela do Modo de espera virtual no servidor do CA ARCserve D2D. Para obter mais informações, consulte o tópico Ligar máquinas virtuais no Modo de espera virtual a partir de instantâneos de pontos de recuperação (na página 85). No entanto, se desejar iniciar máquinas em modo de espera virtual pelo servidor Hyper-V, é possível fazer isso usando o Hyper-V Manager.

Observação: o Hyper-V Manager permite acessar os instantâneos de ponto de recuperação que o CA ARCserve Central Virtual Standby criou para proteger o nó. Você não deve excluir os instantâneos. Ao fazer isso, o relacionamento entre os dados contidos nos instantâneos torna-se inconsistente na próxima vez em que o Modo de espera virtual for executado. Com dados inconsistentes, você não pode ligar a propriedade das máquinas virtuais no Modo de espera virtual.

Para ligar máquinas no modo de espera virtual a partir do Hyper-V Manager

1. Efetue logon no servidor Hyper-V que estiver monitorando os nós que você está protegendo.
2. Inicie o Hyper-V Manager da seguinte maneira:

   Clique em Iniciar, Todos os programas, Ferramentas Administrativas e, em seguida, clique em Gerenciador Hyper-V.

   O Hyper-V Manager é aberto.
3. Na árvore de diretórios, expanda o Gerenciador Hyper-V e clique no servidor Hyper-V contendo a máquina virtual que deseja ligar.

   As máquinas virtuais associadas ao servidor Hyper-V, especificadas na lista de máquinas virtuais, são exibidas no painel central.

4. Siga um destes procedimentos:

   - **Para ligar a máquina virtual usando o instantâneo mais recente**: na lista de máquinas virtuais, clique com o botão direito do mouse na máquina virtual que deseja ligar e clique em Start no menu pop-up.
   - **Para ligar a máquina virtual usando um instantâneo mais antigo:**

     a. Na lista de máquinas virtuais, clique na máquina virtual que deseja ligar.

        Os instantâneos associados à máquina virtual são exibidos na lista Instantâneos.

     b. Clique com o botão direito do mouse no instantâneo que deseja usar para ligar a máquina virtual e clique em Aplicar no menu pop-up.

        A caixa de diálogo Apply Snapshot é aberta.

     c. Clique em Aplicar.

     d. Na lista de máquinas virtuais, clique com o botão direito do mouse na máquina virtual que deseja ligar e clique em Start no menu pop-up.

   A máquina virtual no Modo de espera virtual é ligada.

Se necessário, é possível fazer backup de máquinas virtuais e criar instantâneos de ponto de recuperação depois de ligar a máquina virtual. Para obter mais informações, consulte o tópico Tarefas a serem executadas depois de ligar as máquinas virtuais no Modo de espera virtual.

Ligar máquinas no modo de espera virtual a partir do VMware vSphere Client

Se desejar ligar manualmente máquinas virtuais no Modo de espera virtual, a prática recomendada é ligar as máquinas virtuais pela tela do Modo de espera virtual no servidor do CA ARCserve D2D. Para obter mais informações, consulte o tópico Ligar máquinas virtuais no Modo de espera virtual a partir de instantâneos de pontos de recuperação (na página 85). No entanto, se desejar iniciar máquinas em modo de espera virtual pelo sistema do ESX Server ou vCenter Server, é possível fazer isso usando o VMware vSphere Client.

Observação: o VMware vSphere Client permite acessar os instantâneos de ponto de recuperação que o CA ARCserve Central Virtual Standby criou para proteger o nó. Você não deve excluir os instantâneos. Ao fazer isso, o relacionamento entre os dados contidos nos instantâneos torna-se inconsistente na próxima vez em que o Modo de espera virtual for executado. Com dados inconsistentes, você não pode ligar a propriedade das máquinas virtuais no Modo de espera virtual.

Para ligar máquinas no modo de espera virtual a partir do VMware vSphere Client

1. Abra o VMware vSphere Client e efetue logon no sistema do ESX Server ou vCenter Server que estiver monitorando os nós que você está protegendo.

   Na árvore de diretórios, expanda o sistema do ESX Server ou vCenter Server, localize e clique na máquina virtual que deseja ligar.

2. Siga um destes procedimentos:

   - **Para ligar máquinas virtuais usando o instantâneo mais recente**: clique na guia Introdução e, em seguida, clique em Power on the virtual machine, localizado na parte inferior da tela.
   - **Para ligar a máquina virtual usando um instantâneo mais antigo:**

     a. Clique no botão do gerenciador de instantâneos na barra de ferramentas.

     A caixa de diálogo Snapshots for (nome da máquina virtual) é aberta para exibir uma lista dos instantâneos disponíveis para a máquina virtual.

     b. Na lista de instantâneos, clique no que deseja usar para ligar a máquina virtual e, em seguida, clique em Go to.

   A máquina virtual no Modo de espera virtual é ligada.

Se necessário, é possível fazer backup de máquinas virtuais e criar instantâneos de ponto de recuperação depois de ligar a máquina virtual. Para obter mais informações, consulte o tópico Tarefas a serem executadas depois de ligar as máquinas virtuais no Modo de espera virtual.

Exibir Dados do log de atividades sobre trabalhos

O Virtual Standby permite exibir informações do Log de atividades sobre os trabalhos de Conversão virtual. O Log de atividades contém registros de trabalho de Conversão virtual para os servidores de origem CA ARCserve D2D que estão sendo protegidos.

Observação: o log de atividades (activity.log) é armazenado no seguinte diretório no servidor onde o CA ARCserve D2D está instalado:

```
C:\Arquivos de Programas\CA\ARCserve D2D\Logs
```

Para exibir os dados do Log de atividades sobre trabalhos

1. Abra o Modo de espera virtual e clique em Nós na barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   O CA ARCserve D2D é aberto.

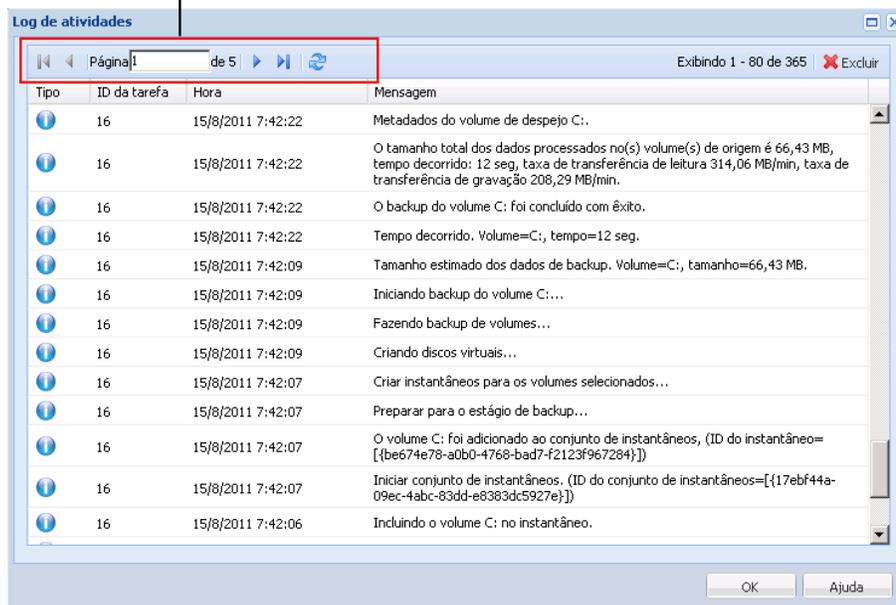
   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

4. Clique na guia Modo de espera virtual.

   A tela Resumo do modo de espera virtual é exibida.

5. (Opcional) Se você estiver conectado a um servidor de monitoramento, expanda Todos ou Servidor em execução na lista de servidores e clique no nó cujo log de atividades deseja exibir.

   Na lista de tarefas de conversão virtual, localizada no lado direito da tela Resumo do modo de espera virtual, clique em Exibir logs.

   A janela Log de atividades é aberta.

Use a barra de navegação para pesquisar e exibir registros do log de atividades. Os ícones abaixo aparecem no Log de atividades:

informações

Aviso

Erro

Observação: para obter informações sobre a exclusão de registros do log de atividades, consulte Excluir registros do log de atividades (na página 91).

Excluir arquivos do Log de atividades

O Virtual Standby permite gerenciar o tamanho geral dos dados do Log de atividades. O log de atividades contém registros de trabalho para os nós de origem do CA ARCserve D2D que estão sendo protegidos. Se você estiver protegendo uma grande quantidade de servidores de origem, ou realiza backups com frequência, ou ambos, o log de atividades pode consumir uma grande quantidade de espaço em disco no nó do CA ARCserve D2D.

Você pode excluir os registros do Log de atividades mais antigos do que uma data especificada ou excluir todos os registros do Log de atividades.

Observação: o log de atividades (activity.log) é armazenado no seguinte diretório no servidor onde o CA ARCserve D2D está instalado:

```
C:\Arquivos de Programas\CA\ARCserve D2D\Logs
```

Para excluir registros do Log de atividades

1. Abra o Modo de espera virtual e clique em Nós na barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   O CA ARCserve D2D é aberto.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

4. Clique na guia Modo de espera virtual.

   A tela Resumo do modo de espera virtual é exibida.

5. (Opcional) Se você estiver conectado a um servidor de monitoramento, expanda Todos ou Servidor em execução na lista de servidores e clique no nó cujo log de atividades deseja excluir.
6. Na lista de tarefas de conversão virtual, localizada no lado direito da tela Resumo do modo de espera virtual, clique em Exibir logs.

   A janela Log de atividades é aberta.
7. Na barra de ferramentas, clique em Excluir.

   A caixa de diálogo Excluir o log de atividades é exibida.
8. Clique em uma das seguintes opções:
   - **Excluir todos os registros de log -** permite excluir todos os registros de tarefa no Log de atividades.

     Observação: use essa opção com cuidado. Você não pode recuperar registros excluídos do Log de atividades.
   - **Excluir todos os registros de log mais antigos que -** permite excluir todos os registros de tarefa no Log de atividades que sejam mais antigos do que a data que você especificar.

   Clique em OK.

Os registros são excluídos do Log de atividades.

Exibir informações de status sobre tarefas do Virtual Standby no servidor do Virtual Standby

O CA ARCserve Central Virtual Standby converte os pontos de recuperação do CA ARCserve D2D em instantâneos do ponto de recuperação. É possível exibir as informações de status sobre as tarefas do Virtual Standby em andamento.

Como alternativa, você pode acessar as informações de status no servidor do Virtual Standby ou diretamente no nó. Para obter informações sobre como acessar as informações de status nos nós, consulte o tópico Exibir informações de status sobre tarefas do Virtual Standby nos nós (na página 93).

Siga estas etapas:

1. Efetue logon no servidor do Virtual Standby.

   Clique em Nós na barra de navegação para abrir a tela Nós.
2. Se houver tarefas do Virtual Standby em andamento, a fase da tarefa será exibida no campo Tarefa, como ilustrado pela seguinte tela:

3. Clique na fase para abrir a caixa de diálogo Monitor de status do Virtual Standby.

   Observação: para obter informações sobre os campos que aparecem no Monitor de status do Virtual Standby, consulte o tópico Monitor de status do Virtual Standby (na página 94).

4. Clique em Fechar para fechar a caixa de diálogo Monitor de status do modo de espera virtual.

Exibir informações de status sobre tarefas do Virtual Standby nos nós

O CA ARCserve Central Virtual Standby converte os pontos de recuperação do CA ARCserve D2D em instantâneos do ponto de recuperação. É possível exibir as informações de status sobre as tarefas de conversão em andamento.

Como alternativa, você pode acessar as informações de status no servidor do Virtual Standby ou diretamente no nó. Para obter informações sobre como acessar informações de status no servidor do Virtual Standby, consulte o tópico Exibir informações de status sobre tarefas do Virtual Standby no servidor do Virtual Standby (na página 92).

Siga estas etapas:

1. Abra o aplicativo e clique em Nós na barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   Você está conectado ao nó do CA ARCserve D2D.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

4. Clique na guia Modo de espera virtual.

   A tela Resumo do modo de espera virtual é exibida.

   Se houver uma tarefa do Virtual Standby em andamento, uma caixa de diálogo de status é exibida no campo Monitor de tarefas, conforme ilustrado a seguir:

5. Clique em Detalhes para abrir o Monitor de status do Virtual Standby.

   Observação: para obter informações sobre os campos que aparecem no Monitor de status do Virtual Standby, consulte o tópico Monitor de status do Virtual Standby (na página 94).

6. Clique em Fechar para fechar a caixa de diálogo Monitor de status do modo de espera virtual.

Monitor de status do Virtual Standby

O Monitor de status do Virtual Standby exibe as seguintes informações em tempo real sobre a tarefa do Virtual Standby:

Fase

Exibe a fase atual do processo de conversão.

Cancelar tarefa

Permite terminar a tarefa de conversão.

Processando

Exibe todo o andamento da tarefa de conversão e o número da sessão do ponto de recuperação que o aplicativo está convertendo.

Ponto de provisionamento atual

Exibe informações de status sobre a sessão que o aplicativo está convertendo.

Sessões de origem

Especifica o número da sessão que o aplicativo está convertendo.

Hora de início

Exibe a data e hora em que o aplicativo foi iniciado para converter a sessão.

Tempo decorrido

Exibe o tempo decorrido desde que o aplicativo iniciou a conversão da sessão atual.

Taxa de transferência

Exibe a taxa na qual o aplicativo está convertendo a sessão.

Tempo restante estimado

Exibe o tempo restante estimado para converter a sessão de origem atual.

Todas as sessões

Exibe informações de status sobre todas as sessões no ponto de recuperação que o aplicativo está convertendo.

Número de sessões convertidas

Exibe o número total de sessões no ponto de provisionamento que foram convertidas.

Tempo decorrido

Exibe o tempo decorrido desde que o aplicativo iniciou a conversão de todas as sessões contidas no ponto de recuperação.

Tempo restante estimado

Exibe o tempo restante estimado para converter todas as sessões contidas no ponto de recuperação.

Número de sessões pendentes

Exibe o número de sessões pendentes para serem convertidas.

Exibir informações sobre diretivas atribuídas a nós do CA ARCserve D2D

O aplicativo permite exibir informações sobre as diretivas de conversão que foram atribuídas aos nós do CA ARCserve D2D.

Para exibir informações sobre diretivas atribuídas a nós do CA ARCserve D2D

1. Abra o aplicativo e clique em Nós na barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   Você está conectado ao nó do CA ARCserve D2D.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

4. Clique na guia Modo de espera virtual.

   A tela Resumo do modo de espera virtual é exibida.

5. Na lista Tarefas em modo de espera virtual, clique em Configurações do modo de espera virtual.

   A caixa de diálogo Configurações do modo de espera virtual é aberta.

   Esta caixa de diálogo permite exibir informações sobre o servidor de virtualização, a máquina virtual, o servidor substituto e as preferências definidas na diretiva que é atribuída ao nó do CA ARCserve D2D. Não é possível editar as diretivas atribuídas ao CA ARCserve D2D da caixa de diálogo Configurações do modo de espera virtual.

   Observação: para obter informações sobre como editar diretivas, consulte o tópico Editar diretivas (na página 56).

6. Clique em Cancelar para fechar a caixa de diálogo Configurações do modo de espera virtual.

Configurações do modo de espera virtual

A caixa de diálogo Configurações do modo de espera virtual contém informações sobre a diretiva atribuída ao nó. Não é possível editar diretivas nessa caixa de diálogo. Para obter mais informações, consulte o tópico Editar diretivas (na página 56).

As seguintes opções são exibidas na guia Modo de espera virtual:

Opções do servidor de virtualização

- **Sistemas VMware:**

  As opções a seguir se aplicam a sistemas VMware:

  - **Tipo de virtualização--**VMware.
  - **Host do ESX/vCenter--**especifica o nome de host do sistema ESX ou vCenter Server.
  - **Nome de usuário--**especifica o nome de usuário necessário para fazer logon no sistema VMware.
  - **Senha--**especifica a senha para o nome de usuário necessária para fazer logon no sistema VMware.
  - **Protocolo--**exibe o protocolo de comunicação usado entre o nó de origem do CA ARCserve D2D e o servidor de monitoramento.
  - **Porta--**especifica a porta usada para a transferência de dados entre o servidor de origem e o servidor de monitoramento.

- **Monitoramento:**

  As opções a seguir se aplicam a sistemas VMware.

  - **Servidor de monitoramento--**especifica o nome do host do servidor que monitora o servidor de origem.
  - **Nome de usuário--**especifica o nome de usuário necessário para fazer logon no sistema VMware.
  - **Senha--**especifica a senha para o nome de usuário necessária para fazer logon no servidor de monitoramento.
  - **Protocolo--**especifica o protocolo de comunicação usado entre o servidor do CA ARCserve Central Virtual Standby e o sistema ESX Server (servidor de monitoramento).
  - **Porta--**especifica a porta usada para a transferência de dados entre o servidor do CA ARCserve Central Virtual Standby e o sistema ESX Server (servidor de monitoramento).
  - **Usar o servidor de monitoramento como proxy para a transferência de dados--**especifica que o servidor de monitoramento copia os dados de conversão do servidor de origem do CA ARCserve D2D para o armazenamento de dados do ESX Server.

    Observação: a opção Usar o servidor de monitoramento como proxy para a transferência de dados fica ativada por padrão. Você pode desativar essa opção para permitir que o servidor CA ARCserve D2D de origem copie os dados de conversão diretamente para o armazenamento de dados do ESX Server.

- **Sistemas Hyper-V:**

  As opções a seguir se aplicam a sistemas Hyper-V:

  - **Tipo de virtualização--**Hyper-V.
  - **Nome do host Hyper-V** - especifica o nome do host do sistema Hyper-V.
  - **Nome de usuário--**especifica o nome de usuário necessário para fazer logon no sistema Hyper-V.
  - **Senha--**especifica a senha para o nome de usuário necessária para fazer logon no sistema Hyper-V.
  - **Porta--**especifica a porta usada para a transferência de dados entre o servidor de origem e o servidor de monitoramento.

Opções de máquina virtual

- **Sistemas VMware:**
  - **Prefixo do nome da VM--**especifica o prefixo adicionado ao nome de exibição da máquina virtual no sistema ESX Server.

    Valor padrão: CAVM_
  - **Pool de recursos da VM--** especifica o nome do pool de recursos no qual a máquina virtual em modo de espera será agrupada.
  - **Armazenamento de dados--** especifica o local onde deseja armazenar os dados de conversão.
    - **Usar um armazenamento de dados para todos os discos de origem da máquina virtual--**especifica que o aplicativo copia todos os discos relacionados à máquina virtual para um armazenamento de dados.
    - **Selecionar um armazenamento de dados para cada disco de origem de VM--**especifica que o aplicativo copia informações relacionadas ao disco da máquina virtual para o armazenamento de dados correspondente.
  - **Redes--**especifica as NICs, redes virtuais e os caminhos que o sistema ESX Server usa para se comunicar com as máquinas virtuais.
    - **Conectar todas as NICs virtuais com a rede virtual--**especifica as NICs virtuais que são mapeadas na rede virtual. Esta opção é especificada quando a máquina virtual contiver NICs virtuais e uma rede virtual.
    - **Selecionar uma rede virtual para cada NIC virtual--**especifica o nome da rede virtual que deseja que a NIC use para se comunicar.
  - **Contagem de CPU--**especifica a contagem mínima e máxima de CPU suportada pela máquina virtual em modo de espera.
  - **Memória -** especifica a quantidade total de RAM (em MB) alocada para a máquina virtual em modo de espera.
- **Sistemas Hyper-V:**
  - **Prefixo do nome da VM--**especifica o prefixo adicionado ao nome de exibição da máquina virtual no sistema Hyper-V.

    Valor padrão: CAVM_
  - **Caminho--**especifica o local no Hyper-v Server onde os dados de conversão são armazenados.
  - **Redes--**especifica as NICs, redes virtuais e os caminhos que o servidor Hyper-V usa para se comunicar com as máquinas virtuais.
  - **Contagem de CPU--**especifica a contagem mínima e máxima de CPU suportada pela máquina virtual em modo de espera.
  - **Memória -** especifica a quantidade total de RAM (em MB) alocada para a máquina virtual em modo de espera.

Configurações substitutas

- **Recuperação:**
  - **Iniciar manualmente a máquina virtual--**especifica que as máquinas virtuais são ligadas e configuradas manualmente quando o servidor de origem falhar ou interromper a comunicação.
  - **Iniciar automaticamente a máquina virtual--**especifica que as máquinas virtuais são ligadas e configuradas automaticamente quando o servidor de origem falhar ou interromper a comunicação.
- **Propriedades do sinal de monitoramento:**
  - **Tempo limite--**especifica o tempo que o servidor de monitoramento deve aguardar um sinal de monitoramento antes de ligar um instantâneo do ponto de recuperação.
  - **Frequência--**especifica a frequência com que o servidor de origem fará a comunicação dos sinais de monitoramento com o servidor do monitor.

As seguintes opções são exibidas na guia Preferências:

- **Alertas por email:**
  - **Sinal de monitoramento ausente na máquina de origem--**especifica que o Virtual Standby envia notificações de alerta quando o servidor de monitoramento não detecta um sinal de monitoramento do servidor de origem.
  - **VM ligada para a máquina de origem configurada para ser ligada automaticamente--**especifica que o Virtual Standby envia notificações de alerta quando ele liga uma máquina virtual que foi configurada para ligar automaticamente quando um sinal de monitoramento não for detectado.
  - **Sinal de monitoramento ausente para a máquina de origem configurada para ser ligada manualmente--**especifica que o Virtual Standby envia notificações de alerta quando não detectar um sinal de monitoramento de um servidor de origem não configurado para ser ligado automaticamente.
  - **Espaço livre de armazenamento da VM abaixo de--** especifica que o Virtual Standby envia notificações de alerta quando detecta espaço livre em disco insuficiente no caminho definido pelo HyperVisor. A detecção ocorre quando a quantidade de espaço livre em disco é menor do que o limite definido pelo usuário. O limite máximo pode ser representado como um valor absoluto (em MB) ou uma porcentagem da capacidade do volume.
  - **Erros/falhas/paralisação no Virtual Standby--**especifica que o Virtual Standby envia notificações de alerta quando detecta um erro que ocorreu durante o processo de conversão.
  - **Operação do Virtual Standby realizada com êxito** - indica que o processo de criação de uma máquina virtual do Virtual Standby foi concluído com êxito.

- **O Hypervisor não está acessível--**especifica que o Virtual Standby envia notificações de alerta quando detecta que ele não pode se comunicar com o sistema ESX Server ou com o sistema Hyper-V.
- **Falha na licença--**especifica que o Virtual Standby envia uma notificação de alerta quando detectar problemas de licenciamento nos servidores do Virtual Standby, servidores de origem e servidores de monitoramento.
- **O Virtual Standby não foi iniciado com êxito a partir do instantâneo do ponto de recuperação** - indica que o processo de criação de uma máquina virtual do Virtual Standby a partir de um instantâneo do ponto de recuperação não foi concluído com êxito.

Como proteger máquinas virtuais do Virtual Standby

Depois que uma máquina virtual do Virtual Standby estiver ligada (manual ou automaticamente), a tarefa de backup do CA ARCserve D2D e a tarefa do Virtual Standby não são executadas da mesma forma que foram programadas. Caso queira retomar as tarefas depois que a máquina virtual do Virtual Standby for ligada, faça o seguinte:

1. Modifique o prefixo do nome da VM na diretiva do Virtual Standby.

   Quando o CA ARCserve Central Virtual Standby liga as máquinas virtuais do Virtual Standby, o aplicativo define os nomes das máquinas virtuais ligadas nas máquinas virtuais de acordo com a opção de prefixo do nome da VM especificada na diretiva do Virtual Standby e o nome do host do nó de origem.

   Exemplo:

   - Prefixo do nome da VM: AA_
   - Nome do host do nó de origem: Server1
   - Nome da máquina virtual da máquina virtual do Virtual Standby: AA_Server1

   Depois que as máquinas virtuais do Virtual Standby estiverem ligadas, pode ocorrer conflitos com o nome da máquina virtual caso o prefixo do nome da VM não seja modificado na diretiva do Virtual Standby. Problemas desse tipo ocorrem quando os nós de origem e as máquinas virtuais do Virtual Standby residirem no mesmo hypervisor.

   Para obter mais informações sobre como modificar o prefixo do nome da VM na diretiva do Virtual Standby, consulte Editar diretivas (na página 56). Se necessário, pode-se atualizar outras configurações de diretivas do Virtual Standby. Opcionalmente, você pode criar uma nova diretiva do Virtual Standby para proteger a máquina virtual do Virtual Standby. Para obter mais informações sobre como criar diretivas, consulte Criar diretivas (na página 30).

2. Depois de atualizar e criar uma diretiva, implante-a na máquina virtual do Virtual Standby. Para obter mais informações, consulte Implantar diretivas (na página 39).
3. Depois de implantar a diretiva na máquina virtual do Virtual Standby, retome a tarefa do Virtual Standby. Para obter mais informações, consulte Pausar e retomar tarefas virtuais no modo de espera (na página 83).
4. Depois de implantar a diretiva, efetue logon no CA ARCserve D2D, na máquina virtual do Virtual Standby e programe um método de repetição para a tarefa de backup do CA ARCserve D2D. Para obter mais informações, consulte o *Guia do Usuário do CA ARCserve D2D*.

Observação: o Gerenciador do CA ARCserve Central Protection e CA ARCserve Central Virtual Standby tem um mecanismo que permite sincronizar automaticamente as diretivas para os nós gerenciados do CA ARCserve D2D semanalmente. Esse mecanismo permite que Gerenciador do CA ARCserve Central Protection reinicie as tarefas de backup nas máquinas virtuais do Virtual Standby implantando novamente a diretiva em vigor no nó do CA ARCserve D2D para a máquina do Virtual Standby. O processo de implantação de diretivas se comporta dessa maneira porque o nó de origem e a máquina virtual do Virtual Standby tem o mesmo nome de host, que permite ao Gerenciador do CA ARCserve Central Protection sincronizar novamente a diretiva. A única limitação para esse comportamento é que o servidor do Gerenciador do CA ARCserve Central Protection e a máquina virtual do Virtual Standby devem ser capazes de se comunicar por meio da rede. Depois que o Gerenciador do CA ARCserve Central Protection sincronizar e implantar a diretiva para a máquina virtual do Virtual Standby, a tarefa do Virtual Standby deve ser retomada na máquina virtual do Virtual Standby. Para obter mais informações, consulte Pausar e retomar tarefas virtuais no modo de espera (na página 83).

Restaurar dados de pontos de recuperação do CA ARCserve D2D

O Virtual Standby permite recuperar dados dos pontos de recuperação disponíveis. Os pontos de recuperação são instantâneos de dados com horário definido que residem em nós de origem do CA ARCserve D2D. A partir dos pontos de recuperação, você pode especificar os dados que deseja recuperar.

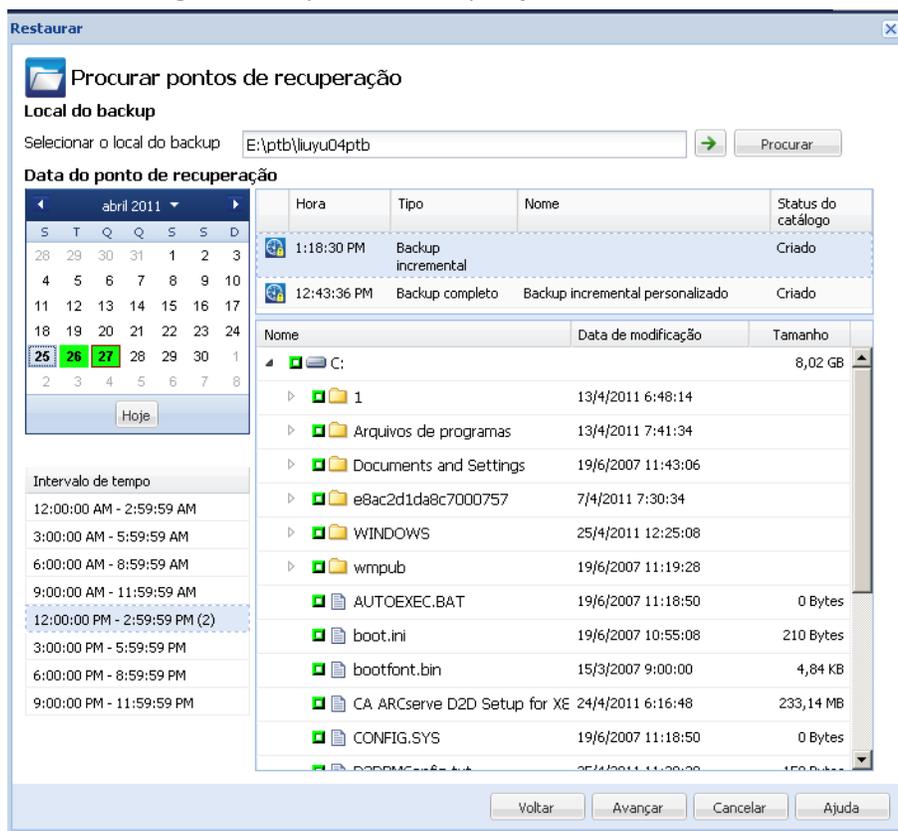
Para restaurar dados dos pontos de recuperação do CA ARCserve D2D

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

2. Na caixa de diálogo Restaurar, clique em Procurar pontos de recuperação.

   A caixa de diálogo Procurar pontos de recuperação é exibida.

3. Especificar a origem do backup. Você pode especificar um local ou procurar o local onde as suas imagens de backup estão armazenadas. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local. Pode-se clicar no ícone de validação em forma de seta verde para confirmar o devido acesso ao local de origem.

   A exibição do calendário realçará (em verde) todas as datas do período exibido que contiverem os pontos de recuperação para essa origem de backup.

4. Especifique os dados que deseja restaurar.

   a. Selecione a data no calendário para a imagem de backup que deseja restaurar.

      Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado e o nome do backup.

   b. Selecione o ponto de recuperação que deseja restaurar.

      O conteúdo do backup correspondente (incluindo aplicativos) para esse ponto de recuperação é exibido.

      Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e que pode ser necessária uma senha para restaurar.

   c. Selecione o conteúdo a ser restaurado.

      - Para uma restauração de nível de volume, pode-se especificar a restauração do volume inteiro ou de arquivos/pastas selecionados no volume.
      - Para uma restauração de nível de aplicativo, é possível especificar a restauração do aplicativo inteiro ou de itens selecionados no aplicativo, como componentes, bancos de dados, instâncias e assim por diante.

5. Depois de especificar os dados que você deseja restaurar, clique em Avançar.

   A caixa de diálogo Opções de restauração é aberta.

6. Preencha as seguintes opções na caixa de diálogo Opções de restauração:

   - **Destino -** selecione o destino da restauração.
     - Restaurar no local original - permite restaurar dados no local original do qual a imagem de backup foi capturada.
     - Restaurar para - permite especificar ou procurar o local em que as imagens de backup serão restauradas. Clique na seta ao lado do campo Restaurar para de forma a verificar a conexão com o local especificado.

       Se necessário, você precisará digitar as credenciais de nome de usuário e senha para obter acesso a esse local.

- **Resolvendo conflitos -** permite especificar como o CA ARCserve D2D deve resolver conflitos encontrados durante o processo de restauração.
  - Substituir os arquivos existentes - permite substituir arquivos existentes que estão localizados no destino de restauração. Todos os objetos serão restaurados nos arquivos de backup, independentemente da presença atual deles em seu computador.
  - Substituir arquivos ativos - permite substituir os arquivos ativos na reinicialização. Se a tentativa de restauração do CA ARCserve D2D detectar que o arquivo existente está em uso, ele não substituirá o arquivo imediatamente. Em vez disso, para evitar problemas, ele atrasará a substituição dos arquivos ativos até a próxima reinicialização do computador. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a reinicialização seguinte.)

    Observação: se essa opção não estiver selecionada, os arquivos ativos serão ignorados na restauração.
  - Renomear arquivos - permite criar novos arquivos se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão, então, restaurados no novo arquivo.
  - Ignorar arquivos existentes - permite ignorar e não substituir arquivos existentes localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

    Por padrão, esta opção está ativada.

- **Estrutura de diretórios -** permite especificar o que o CA ARCserve D2D fará ou não com a estrutura de diretórios durante o processo de restauração.
  - Criar diretório raiz - permite especificar que, se uma estrutura de diretório raiz existir na imagem de backup capturada, o CA ARCserve D2D recriará a mesma estrutura de diretórios raiz no caminho de destino da restauração.

    Quando a opção Criar diretório raiz não estiver selecionada (desmarcada), o arquivo/pasta a ser restaurado será restaurado diretamente na pasta de destino.

    Exemplo:

    Se, durante o backup, você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e, durante a restauração, foi especificado como destino de restauração o local "D:\Restore".

    Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).

    Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

    Quando a opção Criar diretório raiz estiver selecionada (marcada), todo o caminho do diretório raiz até os arquivos/pastas (incluindo o nome do volume) será recriado na pasta de destino. Se os arquivos/pastas a serem restaurados forem do mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

    Exemplo:

    Se, durante o backup, você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e "E:\Pasta3\Subpasta4\C.txt" e, durante a restauração, foi especificado como destino de restauração o local "D:\Restauração".

    Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).

    Se você optar por restaurar tanto o arquivo "A.txt" quanto o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

- **Senha criptografada -** se os dados do ponto de recuperação que você está tentando restaurar estiverem criptografados, poderá ser necessário fornecer a senha criptografada.

  A senha não será obrigatória se estiver tentando restaurar na mesma máquina em que o backup criptografado foi executado. No entanto, se estiver tentando restaurar em uma máquina diferente, a senha será necessária.

  Observação: os ícones a seguir indicam se o ponto de recuperação contém informações criptografadas e poderá exigir uma senha para restauração.

  Ponto de recuperação não criptografado:

  Ponto de recuperação criptografado:

Clique em Avançar.

A caixa de diálogo Resumo de restauração é exibida.

7. Verifique se as informações na caixa de diálogo Resumo da restauração estão corretas.

   Observação: para alterar as opções de restauração especificadas, clique em Voltar e retorne à caixa de diálogo aplicável para alterar os valores.

   Clique em Concluir.

As opções de restauração são aplicadas e os dados são recuperados.

Restaurar dados de cópias de arquivos do CA ARCserve D2D.

O Virtual Standby permite recuperar dados de cópias de arquivos do CA ARCserve D2D. Cópias dos arquivos são cópias de pontos de recuperação do CA ARCserve D2D que você copia para o armazenamento offline, como um disco ou a nuvem. Usando as cópias dos arquivos, você pode especificar os dados que deseja recuperar.

Para restaurar dados de cópias de arquivos do CA ARCserve D2D

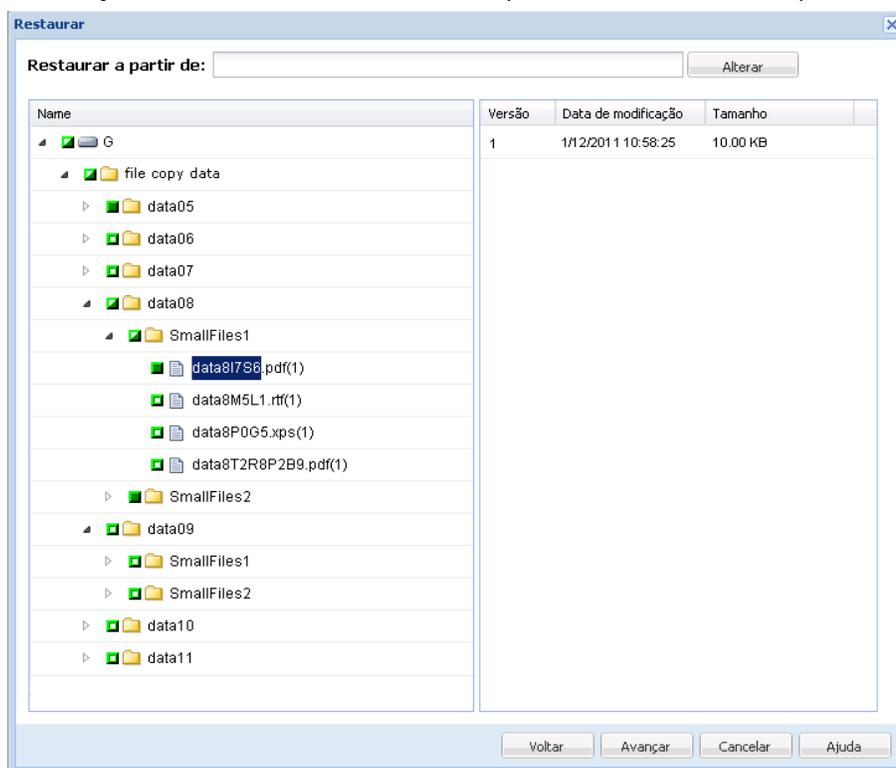
1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

2. Na caixa de diálogo Restaurar, clique em Procurar cópias de arquivo.

   A caixa de diálogo Procurar cópias de arquivo é aberta, conforme ilustrado pela caixa de diálogo a seguir.

   Observação: o destino atualmente exibido no painel à direita é o destino padrão.

3. No painel Nome, especifique os dados da cópia de arquivo que você deseja recuperar. É possível especificar qualquer combinação de arquivos e pastas ou o volume.

   Quando você selecionar um arquivo individual para restauração, todas as versões do arquivo copiado serão exibidas no painel à direita. Se várias versões estiverem disponíveis, selecione a versão de cópia do arquivo que deseja recuperar.

   - **Alterar destino -** permite procurar um local alternativo no qual as imagens de cópias de arquivos estão armazenadas.

     É aberta uma caixa de diálogo que exibe as opções de destino alternativo.

   - **Unidade local ou de rede -** a caixa de diálogo Selecione um local de backup é aberta, permitindo procurar e selecionar uma unidade local ou de rede diferente.

   - **Nuvem -** a caixa de diálogo Configuração de nuvem é aberta, permitindo acessar e selecionar um local de nuvem diferente.

4. Clique em Avançar.

   A caixa de diálogo Opções de restauração é aberta.

5. Preencha as seguintes opções na caixa de diálogo Opções de restauração:

   - **Destino -** selecione o destino da restauração.

     – Restaurar no local original - permite restaurar dados no local original do qual a imagem de backup foi capturada.

     – Restaurar para - permite especificar ou procurar o local em que as imagens de backup serão restauradas. Clique na seta ao lado do campo Restaurar para de forma a verificar a conexão com o local especificado.

       Se necessário, você precisará digitar as credenciais de nome de usuário e senha para obter acesso a esse local.

- **Resolvendo conflitos -** permite especificar como o CA ARCserve D2D deve resolver conflitos encontrados durante o processo de restauração.
  - Substituir os arquivos existentes - permite substituir arquivos existentes que estão localizados no destino de restauração. Todos os objetos serão restaurados nos arquivos de backup, independentemente da presença atual deles em seu computador.
  - Substituir arquivos ativos - permite substituir os arquivos ativos na reinicialização. Se a tentativa de restauração do CA ARCserve D2D detectar que o arquivo existente está em uso, ele não substituirá o arquivo imediatamente. Em vez disso, para evitar problemas, ele atrasará a substituição dos arquivos ativos até a próxima reinicialização do computador. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a reinicialização seguinte.)

    Observação: se essa opção não estiver selecionada, os arquivos ativos serão ignorados na restauração.
  - Renomear arquivos - permite criar novos arquivos se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão, então, restaurados no novo arquivo.
  - Ignorar arquivos existentes - permite ignorar e não substituir arquivos existentes localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

    Por padrão, esta opção está ativada.

- **Estrutura de diretórios -** permite especificar o que o CA ARCserve D2D fará ou não com a estrutura de diretórios durante o processo de restauração.
  - Criar diretório raiz - permite especificar que, se uma estrutura de diretório raiz existir na imagem de backup capturada, o CA ARCserve D2D recriará a mesma estrutura de diretórios raiz no caminho de destino da restauração.

    Quando a opção Criar diretório raiz não estiver selecionada (desmarcada), o arquivo/pasta a ser restaurado será restaurado diretamente na pasta de destino.

    Exemplo:

    Se, durante o backup, você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e, durante a restauração, foi especificado como destino de restauração o local "D:\Restore".

    Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).

    Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

    Quando a opção Criar diretório raiz estiver selecionada (marcada), todo o caminho do diretório raiz até os arquivos/pastas (incluindo o nome do volume) será recriado na pasta de destino. Se os arquivos/pastas a serem restaurados forem do mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

    Exemplo:

    Se, durante o backup, você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e "E:\Pasta3\Subpasta4\C.txt" e, durante a restauração, foi especificado como destino de restauração o local "D:\Restauração".

    Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).

    Se você optar por restaurar tanto o arquivo "A.txt" quanto o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

- **Senha criptografada -** se os dados do ponto de recuperação que você está tentando restaurar estiverem criptografados, poderá ser necessário fornecer a senha criptografada.

  A senha não será obrigatória se estiver tentando restaurar na mesma máquina em que o backup criptografado foi executado. No entanto, se estiver tentando restaurar em uma máquina diferente, a senha será necessária.

  Observação: os ícones a seguir indicam se o ponto de recuperação contém informações criptografadas e poderá exigir uma senha para restauração.

  Ponto de recuperação não criptografado:

  Ponto de recuperação criptografado:

Clique em Avançar.

A caixa de diálogo Resumo de restauração é exibida.

6. Verifique se as informações na caixa de diálogo Resumo da restauração estão corretas.

   Observação: para alterar as opções de restauração especificadas, clique em Voltar e retorne à caixa de diálogo aplicável para alterar os valores.

   Clique em Concluir.

As opções de restauração são aplicadas e os dados são recuperados.

Restaurar dados usando a opção Localizar arquivos/pastas para restauração

O Virtual Standby permite pesquisar pontos de recuperação e cópias de arquivos do CA ARCserve D2D para restaurar arquivos ou pastas específicos.

Para restaurar dados usando a opção Localizar arquivos/pastas para restauração

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

2. Na caixa de diálogo Restaurar, clique em Localizar arquivos/pastas para restauração.

   A caixa de diálogo Localizar arquivos/pastas para restauração é exibida.

3. Especifique onde pesquisar (backup e/ou origem da cópia de arquivo).

   É possível especificar um local ou procurar o local onde as suas imagens de backup/cópia de arquivo estão armazenadas. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local. Pode-se clicar no ícone de validação em forma de seta verde para confirmar o devido acesso ao local de origem.

4. Especifique o que pesquisar (nome do arquivo ou pasta a ser restaurado).

   Observação: o campo Nome de arquivo oferece suporte a pesquisa de nome completo e pesquisa com caracteres curinga. Se não souber o nome do arquivo completo, é possível simplificar os resultados da pesquisa especificando os caracteres curinga "*" e "?" no campo Nome de arquivo.

   Os caracteres curinga suportados para o nome de arquivo ou pasta são os seguintes:

   - "*" -- use o asterisco para substituir zero ou mais caracteres em um nome de arquivo ou pasta.
   - "?" -- use o ponto de interrogação para substituir um único caractere em um nome de arquivo ou pasta.

   Por exemplo, se *.txt for especificado, todos os arquivos com uma extensão de arquivo .txt serão exibidos nos resultados da pesquisa.

   Observação: se necessário, você também pode especificar um caminho para o filtro de pesquisa e selecionar se deseja incluir ou não os subdiretórios.

5. Clique em Localizar para iniciar a pesquisa.

   Os resultados da pesquisa são exibidos. Se a pesquisa detectar várias ocorrências (pontos de recuperação) do mesmo arquivo pesquisado, ela listará todas as ocorrências classificadas por data (com a mais recente listada primeiro). Ele também indicará se o arquivo pesquisado foi submetido a backup ou foi arquivado.

6. Selecione a versão (ocorrência) do arquivo/pasta que deseja restaurar e clique em Avançar.

   A caixa de diálogo Opções de restauração é aberta.

7. Preencha as seguintes opções na caixa de diálogo Opções de restauração:

   - **Destino -** selecione o destino da restauração.
     - Restaurar no local original - permite restaurar dados no local original do qual a imagem de backup foi capturada.
     - Restaurar para - permite especificar ou procurar o local em que as imagens de backup serão restauradas. Clique na seta ao lado do campo Restaurar para de forma a verificar a conexão com o local especificado.

       Se necessário, você precisará digitar as credenciais de nome de usuário e senha para obter acesso a esse local.

- **Resolvendo conflitos -** permite especificar como o CA ARCserve D2D deve resolver conflitos encontrados durante o processo de restauração.
  - Substituir os arquivos existentes - permite substituir arquivos existentes que estão localizados no destino de restauração. Todos os objetos serão restaurados nos arquivos de backup, independentemente da presença atual deles em seu computador.
  - Substituir arquivos ativos - permite substituir os arquivos ativos na reinicialização. Se a tentativa de restauração do CA ARCserve D2D detectar que o arquivo existente está em uso, ele não substituirá o arquivo imediatamente. Em vez disso, para evitar problemas, ele atrasará a substituição dos arquivos ativos até a próxima reinicialização do computador. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a reinicialização seguinte.)

    Observação: se essa opção não estiver selecionada, os arquivos ativos serão ignorados na restauração.
  - Renomear arquivos - permite criar novos arquivos se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão, então, restaurados no novo arquivo.
  - Ignorar arquivos existentes - permite ignorar e não substituir arquivos existentes localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

    Por padrão, esta opção está ativada.

- **Estrutura de diretórios -** permite especificar o que o CA ARCserve D2D fará ou não com a estrutura de diretórios durante o processo de restauração.

  – Criar diretório raiz - permite especificar que, se uma estrutura de diretório raiz existir na imagem de backup capturada, o CA ARCserve D2D recriará a mesma estrutura de diretórios raiz no caminho de destino da restauração.

    Quando a opção Criar diretório raiz não estiver selecionada (desmarcada), o arquivo/pasta a ser restaurado será restaurado diretamente na pasta de destino.

    Exemplo:

    Se, durante o backup, você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e, durante a restauração, foi especificado como destino de restauração o local "D:\Restore".

    Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).

    Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

    Quando a opção Criar diretório raiz estiver selecionada (marcada), todo o caminho do diretório raiz até os arquivos/pastas (incluindo o nome do volume) será recriado na pasta de destino. Se os arquivos/pastas a serem restaurados forem do mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

    Exemplo:

    Se, durante o backup, você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e "E:\Pasta3\Subpasta4\C.txt" e, durante a restauração, foi especificado como destino de restauração o local "D:\Restauração".

    Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).

    Se você optar por restaurar tanto o arquivo "A.txt" quanto o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

- **Senha criptografada -** se os dados do ponto de recuperação que você está tentando restaurar estiverem criptografados, poderá ser necessário fornecer a senha criptografada.

  A senha não será obrigatória se estiver tentando restaurar na mesma máquina em que o backup criptografado foi executado. No entanto, se estiver tentando restaurar em uma máquina diferente, a senha será necessária.

  Observação: os ícones a seguir indicam se o ponto de recuperação contém informações criptografadas e poderá exigir uma senha para restauração.

  Ponto de recuperação não criptografado:

  Ponto de recuperação criptografado:

Clique em Avançar.

A caixa de diálogo Resumo de restauração é exibida.

8. Verifique se as informações na caixa de diálogo Resumo da restauração estão corretas.

   Observação: para alterar as opções de restauração especificadas, clique em Voltar e retorne à caixa de diálogo aplicável para alterar os valores.

   Clique em Concluir.

As opções de restauração são aplicadas e os dados são recuperados.

Recuperar servidores de origem usando recuperação bare metal

Depois de corrigir os problemas ou executar manutenção em seus servidores de origem, o Virtual Standby permite recuperar os servidores de origem para o último estado íntegro e incluir alterações incrementais que ocorreram enquanto o Instantâneo do ponto de recuperação era ligado.

O processo de recuperação é chamado de recuperação V2P (virtual para físico).

O processo de recuperação V2P aproveita o processo de recuperação bare metal (BMR) do CA ARCserve D2D para restaurar dados de máquinas virtuais para computadores físicos. A recuperação bare metal é o processo de restauração de um sistema de computador do estado de simples metal, incluindo a reinstalação do sistema operacional e dos aplicativos de software e, em seguida, a restauração dos dados e das configurações.

Antes de executar a BMR, é preciso ter:

- Um dos seguintes itens:
  - Uma imagem personalizada do Windows PE (D2DBMR.ISO) fornecida juntamente com o CA ARCserve D2D.
  - Um dispositivo USB de BMR criado pelo assistente do kit de inicialização, juntamente com a mídia de instalação (CD/DVD) do Windows 7/Windows Vista/Windows 2008/Windows 2008R2. (O dispositivo USB também pode ser usado com a imagem do Windows PE em vez da mídia de instalação para carregar os drivers necessários durante a BMR, se for preciso).

    Observação: ao usar um dispositivo USB, é possível adicionar mais drivers a ele, o que não se pode fazer com a imagem do Windows PE.
- Ao menos um backup completo disponível.
- Uma RAM de ao menos 1 GB instalada na máquina virtual e o servidor de origem que se está recuperando.
- Para recuperar máquinas virtuais VMware para máquinas virtuais VMware configuradas para se comportarem como servidores físicos, verifique se o VMware Tools está instalado na máquina virtual de destino.

Discos dinâmicos serão restaurados somente no nível do disco. Se o backup dos dados for feito no volume local de um disco dinâmico, você não poderá restaurar este disco durante a BMR. Nesse cenário, para fazer uma restauração durante uma BMR, é preciso executar uma das tarefas abaixo e, em seguida, realizar a BMR a partir do ponto de recuperação copiado:

- Faça backup em um volume em outra unidade.
- Faça backup em um compartilhamento remoto.
- Copie um ponto de recuperação em outro local.

Observação: se executar uma BMR em um disco dinâmico, não execute nenhuma operação no disco antes da BMR (como limpeza ou exclusão de volume) ou a presença do disco pode não ser reconhecida.

Independentemente do método usado para criar a imagem do kit de inicialização, o processo de BMR é basicamente o mesmo.

O aplicativo permite recuperar dados usando os métodos descritos na tabela a seguir:

Método de recuperação	**Mais informações**
Recuperar servidores de origem de dados dos armazenados em backup usando o CA ARCserve D2D.	Recuperar servidores de origem usando os dados de backup do CA ARCserve D2D (na página 118).

Método de recuperação	Mais informações
Recuperar servidores de origem de dados que foram convertidos em máquinas virtuais em modo de espera virtual com base no Hyper-V.	Recuperar servidores de origem usando dados de máquinas virtuais em modo de espera virtual no Hyper-V (na página 134).
Recuperar servidores de origem de dados que foram convertidos em máquinas virtuais em modo de espera virtual com base no VMware.	Recuperar servidores de origem usando dados de máquinas virtuais em modo de espera virtual no VMware (na página 148).

Recuperar servidores de origem usando os dados de backup do CA ARCserve D2D

O aplicativo permite a recuperação de servidores de origem de dados armazenados em backup usando o CA ARCserve D2D.

Observação: o aplicativo usa o processo de recuperação bare metal para recuperar servidores de origem de dados de backup do CA ARCserve D2D. Para obter mais informações, consulte o tópico Recuperando servidores de origem usando uma recuperação bare metal (na página 116).

Para recuperar servidores de origem usando os dados de backup do CA ARCserve D2D

1. Insira a mídia da imagem do kit de inicialização salva e inicialize o computador.
   - Se estiver usando uma imagem salva do Windows PE, insira o CD/DVD da imagem do kit de inicialização.
   - Se estiver usando um dispositivo USB, insira o CD/DVD de instalação do Windows Server e conecte o dispositivo USB contendo a imagem salva do kit de inicialização.

   A tela do utilitário de instalação do BIOS é exibida.

2. Nessa tela, selecione a opção da unidade de CD-ROM para abrir o processo de inicialização.

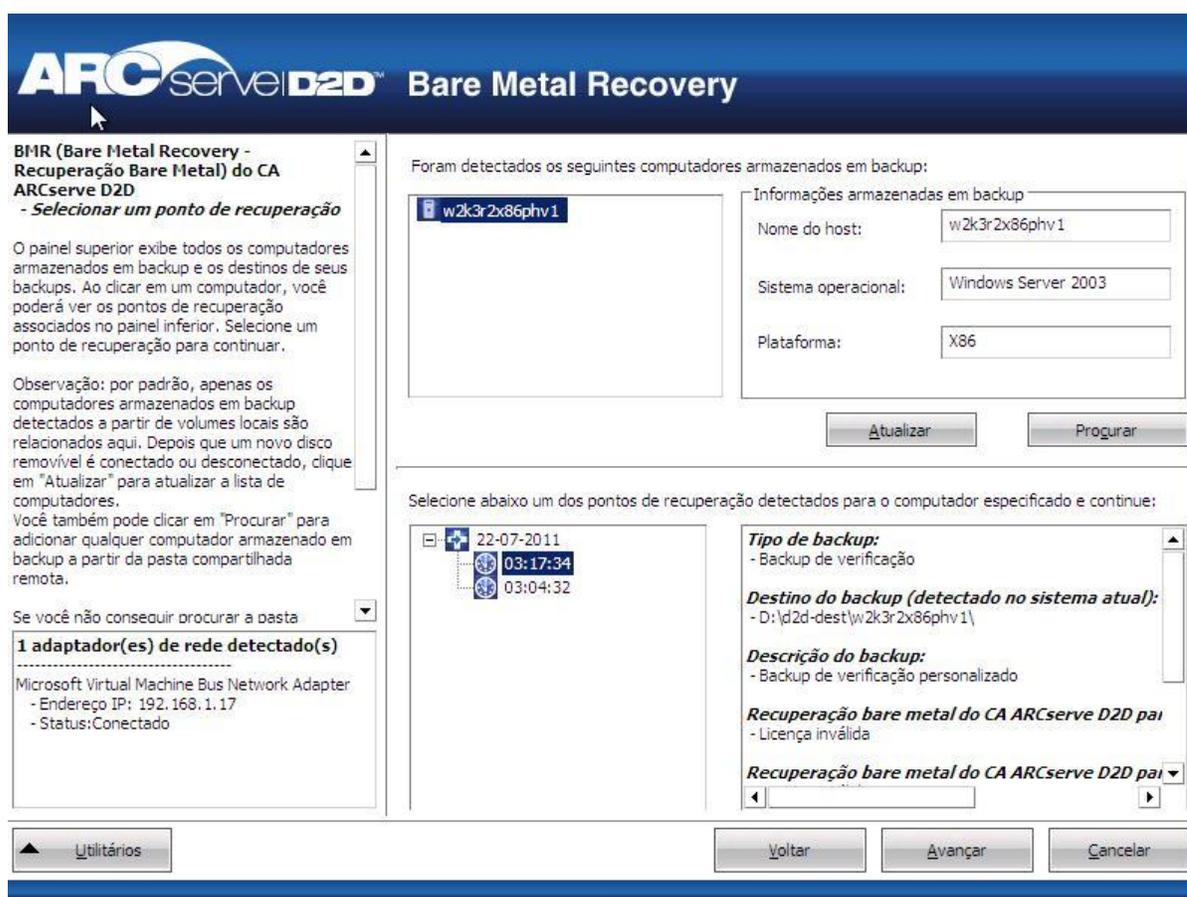
   Observação: se estiver usando a imagem do Windows PE para executar uma BMR, selecione uma arquitetura (x86/x64) e pressione Enter para continuar.

3. A tela de seleção de idioma do CA ARCserve D2D é exibida. Selecione um idioma e clique em Avançar para continuar.

   Observação: se executar uma BMR com um USB e uma mídia de instalação do Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 (CD/DVD) sem suporte a MUI (Multilingual User Interface - Interface de Usuário Multilíngue), a tela de seleção de idioma não será exibida.

O processo de recuperação bare metal é iniciado, e a tela do assistente da BMR inicial é exibida.

4. Clique em Recuperar dados armazenados em backup usando o CA ARCserve D2D e, em seguida, clique em Avançar.

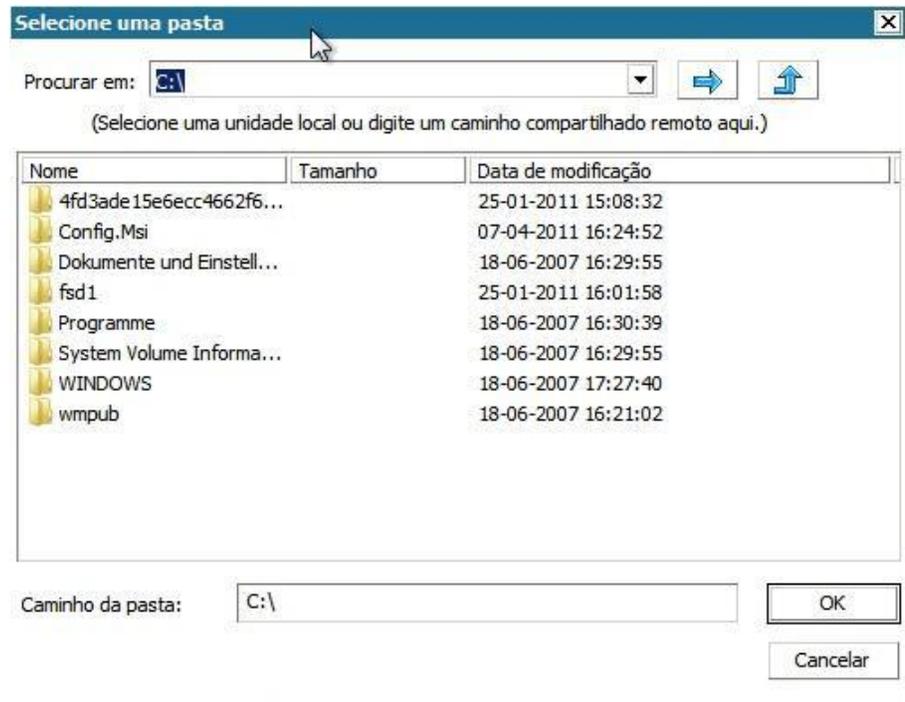
   A tela do assistente Selecionar um ponto de recuperação é exibida.

5. Nesta tela, selecione o computador (ou volume) que contenha pontos de recuperação para a imagem de backup.

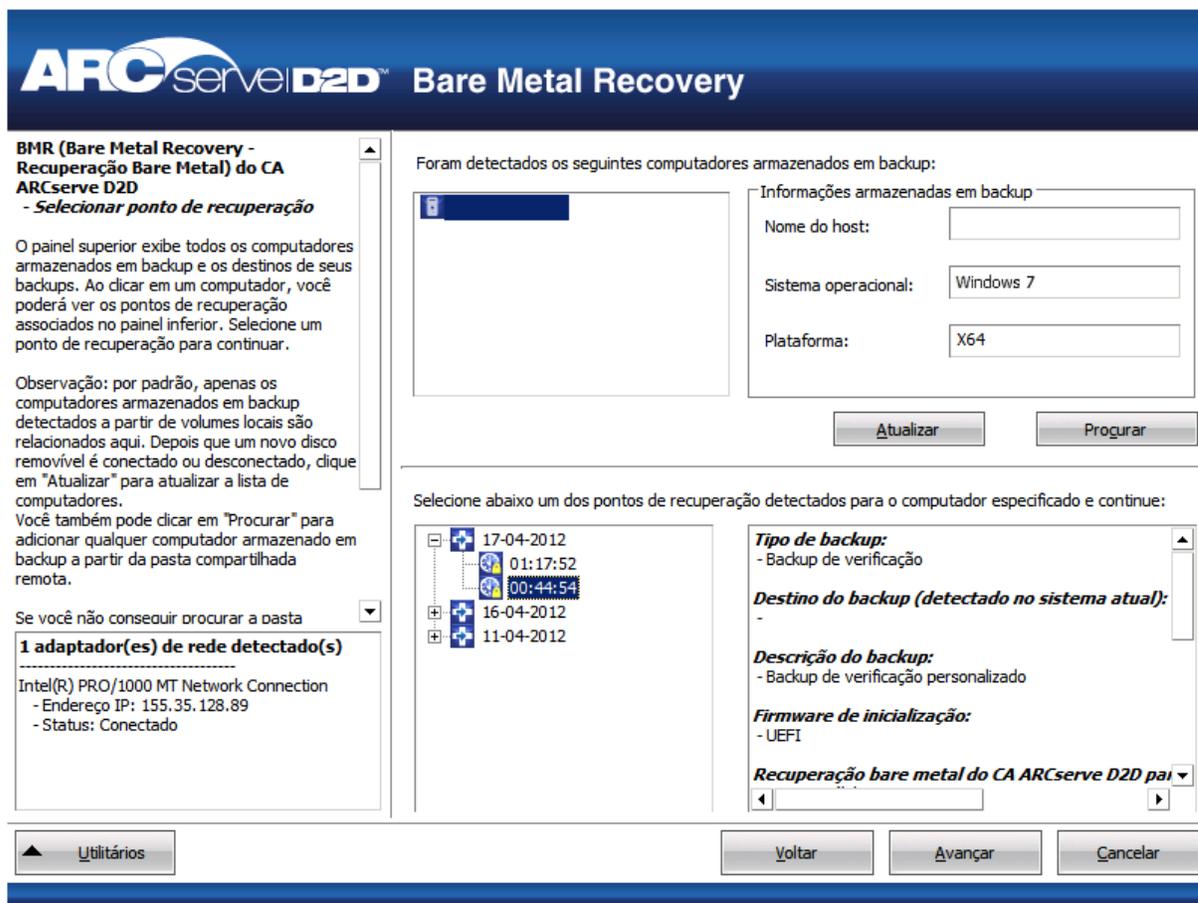
   O CA ARCserve D2D permite recuperar a partir de uma unidade local ou compartilhamento de rede.

   - Se você estiver recuperando a partir de um backup local, o assistente de BMR detectará e exibirá automaticamente todos os volumes contendo pontos de recuperação.
   - Caso esteja fazendo uma recuperação a partir de um compartilhamento remoto, é preciso procurar o local remoto onde os pontos de recuperação estão armazenados. Se houver vários computadores contendo pontos de recuperação, todos eles serão exibidos.

     Você também pode precisar acessar informações (nome de usuário e senha) para o computador remoto.

     Observação: a rede deve estar em funcionamento para procurar pontos de recuperação. Se necessário, você pode verificar e atualizar as informações de configuração de rede ou carregar qualquer driver ausente do menu Utilitários.

6. Se o módulo de BMR não conseguir detectar um volume de destino local, a caixa de diálogo Selecionar uma pasta é exibida automaticamente, e será necessário fornecer o compartilhamento remoto onde os backups residem.

7. Selecione a pasta onde estão armazenados os pontos de recuperação para backup e clique em OK. (Você pode clicar no ícone de seta verde para validar a conexão com o local especificado.)

   A tela do assistente de BMR agora exibe o nome do computador (no painel superior à esquerda), juntamente com informações do backup em questão (no painel superior à direita) e todos os pontos de recuperação correspondentes (no painel inferior à esquerda).

8. Selecione o ponto de recuperação a ser restaurado.

   As informações relacionadas ao ponto de recuperação selecionado são exibidas (no painel inferior à direita). Essa exibição inclui informações como o tipo de backup executado (e salvo), o destino do backup e os volumes incluídos no backup.

   Se o ponto de recuperação contiver sessões criptografadas (o ícone de relógio do ponto de recuperação terá um cadeado), uma tela de senha obrigatória será exibida. Digite a senha da sessão e clique em OK.

   Observação: se seu computador for um controlador de domínio, o CA ARCserve D2D oferece suporte a uma restauração não autoritativa do arquivo de banco de dados do AD (Active Directory) durante a BMR. (Não há suporte à restauração de clusters do MSCS).

9. Verifique se este é o ponto de recuperação que deseja restaurar e clique em Avançar.

   Uma tela do assistente de BMR é exibida com as opções disponíveis do modo de recuperação.

10. Selecione o modo de recuperação.

    As opções disponíveis são Modo avançado e Modo expresso.

    - Selecione o Modo avançado, caso deseje personalizar o processo de recuperação.
    - Selecione o Modo expresso, se desejar o mínimo de interação durante o processo de recuperação.

    Padrão: Modo expresso.

    Observação: o restante desse procedimento é aplicável apenas se o modo avançado for selecionado e se o procedimento fornecer informações para orientá-lo durante o processo da BMR.

11. Clique em Avançar.

    O utilitário BMR inicia localizando o computador a ser recuperado e exibe as informações da partição de disco correspondente.

    O painel superior mostra a configuração de disco que você possui no computador atual (destino) e o painel inferior mostra as informações da partição de disco que havia no computador original (origem).

Importante: Um ícone vermelho em forma de X exibido para um volume de origem no painel inferior indica que o volume contém informações do sistema e não foi atribuído (mapeado) ao volume de destino. O volume contendo informações do sistema do disco de origem deve ser atribuído ao disco de destino e restaurado durante a BMR, caso contrário, haverá falha na reinicialização.

Observação: se executar a BMR e restaurar o volume do sistema em um disco que não está configurado como disco de inicialização, haverá falha ao iniciar o computador após o término da BMR. Verifique se está restaurando o volume do sistema em um disco de inicialização configurado corretamente.

Observação: ao restaurar em outro disco/volume, a capacidade do novo disco/volume deve ser do mesmo tamanho ou maior do que o disco/volume original. Além disso, o redimensionamento do disco destina-se somente a discos básicos, não a discos dinâmicos.

12. Se as informações do disco atual que você estiver vendo não parecem corretas, acesse o menu Utilitários e verifique se há drivers ausentes.

13. Se necessário, no painel de volume do destino, clique no menu suspenso Operações para exibir as opções disponíveis.

    Nesse menu, é possível redefinir as partições existentes ou criar partições que correspondam às partições de disco no volume de origem. (Redefinir significa recarregar as informações de layout do disco de origem e de destino a partir do arquivo de configuração e do sistema operacional atual, e descartar quaisquer informações de layout de disco alteradas pelo usuário).

    Observação: ao fazer mapeamento para outro disco, a capacidade de cada volume de destino mapeado deve ser do mesmo tamanho ou maior do que o volume de origem correspondente.

14. Clique em cada volume de destino e, no menu pop-up, selecione a opção Mapear volume de para atribuir um volume de origem a este volume de destino.

    A caixa de diálogo Selecionar um volume de origem básico é exibida.

15. Nesta caixa, clique no menu suspenso e selecione o volume de origem disponível para atribuí-lo ao volume de destino selecionado. Clique em OK.

    - No volume de destino, um ícone de marca de seleção é exibido, indicando que o volume de destino foi mapeado.
    - No volume de origem, o ícone em forma de X vermelho muda para verde, indicando que o volume de origem foi atribuído a um volume de destino.

16. Quando tiver certeza de que todos os volumes que desejar restaurar e todos os volumes que tiverem informações do sistema foram atribuídos a um volume de destino, clique em Avançar.

    A tela Enviar alterações de disco é exibida, mostrando um resumo das operações selecionadas. Para cada novo volume criado, são exibidas as informações correspondentes.

17. Ao confirmar se as informações de resumo estão corretas, clique em Enviar. (Se não estiverem corretas, clique em Cancelar.)

    Observação: as operações no disco rígido não entrarão em vigor até que sejam enviadas.

    No computador de destino, os novos volumes são criados e mapeados para o computador de origem correspondente.

18. Quando as alterações forem concluídas, clique em OK.

    A tela Resumo das configurações de restauração é exibida, mostrando um resumo dos volumes a serem restaurados.

    Observação: na parte inferior da janela de resumo da restauração, as letras de unidade listadas na coluna Volume de destino são geradas automaticamente no WinPE (Windows Preinstallation Environment - Ambiente de Pré-Instalação do Windows). Elas podem ser diferentes das listadas na coluna Volume de origem. No entanto, os dados serão restaurados no volume apropriado, mesmo quando as letras forem diferentes.

19. Após verificar se as informações de resumo estão corretas, clique em OK.

    O processo de restauração é iniciado. A tela do assistente de BMR exibe o status da restauração para cada volume.

    - Dependendo do tamanho do volume sendo restaurado, essa operação pode levar algum tempo.
    - Durante este processo, você estará restaurando bloco por bloco tudo o que tiver sido armazenado em backup para esse ponto de recuperação e criando uma réplica do computador de origem no computador de destino.
    - Por padrão, a opção que permite reiniciar o sistema automaticamente depois da recuperação é selecionada. Se necessário, você pode desmarcar esta opção e reinicializar manualmente mais tarde.
    - Se necessário, é possível cancelar ou anular a operação a qualquer momento.

20. No menu Utilitários, é possível acessar o Log de atividades da BMR e usar a opção Salvar para salvar o Log de atividades.

    Por padrão, o log de atividades será salvo no seguinte local:

    X:\windows\system32\dr\log.

    Observação: para evitar um erro gerado pelo Windows, não salve o Log de atividades na área de trabalho nem crie uma nova pasta na área de trabalho usando a opção Salvar como, na janela Log de atividades da BMR.

21. Caso esteja restaurando em diferentes tipos de hardware (o adaptador SCSI/FC usado para conectar unidades de disco rígido pode ter sido alterado) e nenhum driver compatível tenha sido detectado no sistema original, uma página de injeção de drivers será exibida para permitir o fornecimento de drivers a esses dispositivos.

    Procure e selecione os drivers a serem injetados no sistema recuperado de forma que, mesmo se estiver fazendo a recuperação em um computador com tipos diferentes de hardware, ainda seja possível trazer o computador de volta após a BMR.

22. Quando o processo de BMR for concluído, uma notificação de confirmação é exibida.

Observações: após a conclusão da BMR:

- O primeiro backup realizado é o Backup de verificação.
- Verifique se a BIOS está configurada para inicializar a partir do disco no qual o volume de inicialização foi restaurado.
- Após a reinicialização do computador, talvez seja necessário configurar os adaptadores de rede manualmente caso você tenha restaurado em um hardware diferente.
- Para discos dinâmicos, se o status do disco for offline, é possível alterá-lo manualmente para online na interface de gerenciamento de disco (acessado executando o utilitário de controle Diskmgmt.msc).
- Para discos dinâmicos, se os volumes dinâmicos estiverem em um status de falha de redundância, é possível sincronizar novamente os volumes na interface de gerenciamento de disco (acessado usando o utilitário de controle Diskmgmt.msc).

Recuperar servidores de origem usando dados de máquinas virtuais em modo de espera virtual no Hyper-V

O aplicativo permite a recuperação de servidores de origem usando dados do CA ARCserve D2D que foram convertidos em máquinas virtuais em modo de espera virtual no Hyper-V.

Observação: o aplicativo usa o processo de recuperação bare metal para recuperar servidores de origem máquinas virtuais do Hyper-V. Para obter mais informações, consulte o tópico Recuperando servidores de origem usando uma recuperação bare metal (na página 116).

Para recuperar servidores de origem usando dados de máquinas virtuais em modo de espera virtual no Hyper-V.

1. Insira a mídia da imagem do kit de inicialização salva e inicialize o computador.
   - Se estiver usando uma imagem salva do Windows PE, insira o CD/DVD da imagem do kit de inicialização.
   - Se estiver usando um dispositivo USB, insira o CD/DVD de instalação do Windows Server e conecte o dispositivo USB contendo a imagem salva do kit de inicialização.

   A tela do utilitário de instalação do BIOS é exibida.

2. Nessa tela, selecione a opção da unidade de CD-ROM para abrir o processo de inicialização.

   Observação: se estiver usando a imagem do Windows PE para executar uma BMR, selecione uma arquitetura (x86/x64) e pressione Enter para continuar.

3. A tela de seleção de idioma do CA ARCserve D2D é exibida. Selecione um idioma e clique em Avançar para continuar.

   Observação: se executar uma BMR com um USB e uma mídia de instalação do Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 (CD/DVD) sem suporte a MUI (Multilingual User Interface - Interface de Usuário Multilíngue), a tela de seleção de idioma não será exibida.

O processo de recuperação bare metal é iniciado, e a tela do assistente da BMR inicial é exibida.

4. Após selecionar a tela do assistente Selecionar o tipo de BMR (Bare Metal Recovery - Recuperação Bare Metal), selecione a opção Recuperar usando uma VM no modo de espera virtual do Hyper-V.

BMR (Bare Metal Recovery - Recuperação Bare Metal) do CA ARCserve D2D
- Escolha um tipo de BMR

Especifique um tipo de recuperação:

○ **Recuperar dados cujo backup foi feito usando o CA ARCserve D2D**

(Sessões de backup usando o CA ARCserve D2D ou CA ARCserve Central Host-Based VM Backup).

◉ **Recuperar usando uma VM no modo de espera virtual do Hyper-V**

(é possível recuperar dados apenas se a conversão virtual tiver sido feita usando o CA ARCserve Central Virtual Standby)

○ **Recuperar usando uma VM no modo de espera virtual do VMware**

(é possível recuperar dados apenas se a conversão virtual tiver sido feita usando o CA ARCserve Central Virtual Standby)

5. Clique em Avançar.

   A tela Selecione o instantâneo de uma máquina virtual é exibida, com a caixa de diálogo autenticação do Hyper-V, solicitando detalhes do servidor Hyper-V.

6. Digite as informações de autenticação e clique em OK.

   O CA ARCserve D2D detecta e exibe o Hyper-V Server com uma lista de todas as máquinas virtuais que são convertidas no servidor Hyper-V especificado usando o CA ARCserve Central Virtual Standby.

7. Selecione a máquina virtual que contém os instantâneos do ponto de recuperação para a imagem de backup.

   As sessões de backup (instantâneos do ponto de recuperação) da máquina virtual selecionada são exibidas.

8. Selecione a sessão de backup da máquina virtual (instantâneo do ponto de recuperação) que deseja recuperar.

   Os detalhes correspondentes do instantâneo do ponto de recuperação selecionado (nome da máquina virtual, nome da sessão de backup, volumes armazenados em backup) são exibidos no painel direito.

   Além disso, para selecionar um dos pontos de recuperação relacionados, tem-se também a opção de selecionar o ponto de recuperação do estado atual ou do estado mais recente.

   - Se a máquina virtual que estiver recuperando estiver ligada, o ponto de recuperação do estado atual é exibido.
   - Se a máquina virtual que estiver recuperando estiver desligada, o ponto de recuperação do estado mais recente é exibido.

     Se selecionar o ponto de recuperação do estado mais recente, uma mensagem de erro será exibida para informar que o ponto de recuperação que você está recuperando é o estado mais recente (e não o atual) e solicitando que se inicie a máquina virtual antes de continuar com o processo de recuperação.

9. Verifique se este é o ponto de recuperação que deseja restaurar e clique em Avançar.

   Uma tela do assistente de BMR é exibida com as opções disponíveis do modo de recuperação.

10. Selecione o modo de recuperação.

    As opções disponíveis são Modo avançado e Modo expresso.

    - Selecione o Modo avançado, caso deseje personalizar o processo de recuperação.
    - Selecione o Modo expresso, se desejar o mínimo de interação durante o processo de recuperação.

    Padrão: Modo expresso.

    Observação: o restante desse procedimento é aplicável apenas se o modo avançado for selecionado e se o procedimento fornecer informações para orientá-lo durante o processo da BMR.

11. Clique em Avançar.

    O utilitário BMR inicia localizando o computador a ser recuperado e exibe as informações da partição de disco correspondente.

    O painel superior mostra a configuração de disco que você possui no computador atual (destino) e o painel inferior mostra as informações da partição de disco que havia no computador original (origem).

Importante: Um ícone vermelho em forma de X exibido para um volume de origem no painel inferior indica que o volume contém informações do sistema e não foi atribuído (mapeado) ao volume de destino. O volume contendo informações do sistema do disco de origem deve ser atribuído ao disco de destino e restaurado durante a BMR, caso contrário, haverá falha na reinicialização.

Observação: se executar a BMR e restaurar o volume do sistema em um disco que não está configurado como disco de inicialização, haverá falha ao iniciar o computador após o término da BMR. Verifique se está restaurando o volume do sistema em um disco de inicialização configurado corretamente.

Observação: ao restaurar em outro disco/volume, a capacidade do novo disco/volume deve ser do mesmo tamanho ou maior do que o disco/volume original. Além disso, o redimensionamento do disco destina-se somente a discos básicos, não a discos dinâmicos.

12. Se as informações do disco atual que você estiver vendo não parecem corretas, acesse o menu Utilitários e verifique se há drivers ausentes.

13. Se necessário, no painel de volume do destino, clique no menu suspenso Operações para exibir as opções disponíveis.

    Nesse menu, é possível redefinir as partições existentes ou criar partições que correspondam às partições de disco no volume de origem. (Redefinir significa recarregar as informações de layout do disco de origem e de destino a partir do arquivo de configuração e do sistema operacional atual, e descartar quaisquer informações de layout de disco alteradas pelo usuário).

    Observação: ao fazer mapeamento para outro disco, a capacidade de cada volume de destino mapeado deve ser do mesmo tamanho ou maior do que o volume de origem correspondente.

14. Clique em cada volume de destino e, no menu pop-up, selecione a opção Mapear volume de para atribuir um volume de origem a este volume de destino.

    A caixa de diálogo Selecionar um volume de origem básico é exibida.

15. Nesta caixa, clique no menu suspenso e selecione o volume de origem disponível para atribuí-lo ao volume de destino selecionado. Clique em OK.

    - No volume de destino, um ícone de marca de seleção é exibido, indicando que o volume de destino foi mapeado.
    - No volume de origem, o ícone em forma de X vermelho muda para verde, indicando que o volume de origem foi atribuído a um volume de destino.

16. Quando tiver certeza de que todos os volumes que desejar restaurar e todos os volumes que tiverem informações do sistema foram atribuídos a um volume de destino, clique em Avançar.

    A tela Enviar alterações de disco é exibida, mostrando um resumo das operações selecionadas. Para cada novo volume criado, são exibidas as informações correspondentes.

17. Ao confirmar se as informações de resumo estão corretas, clique em Enviar. (Se não estiverem corretas, clique em Cancelar.)

    Observação: as operações no disco rígido não entrarão em vigor até que sejam enviadas.

    No computador de destino, os novos volumes são criados e mapeados para o computador de origem correspondente.

18. Quando as alterações forem concluídas, clique em OK.

    A tela Resumo das configurações de restauração é exibida, mostrando um resumo dos volumes a serem restaurados.

    Observação: na parte inferior da janela de resumo da restauração, as letras de unidade listadas na coluna Volume de destino são geradas automaticamente no WinPE (Windows Preinstallation Environment - Ambiente de Pré-Instalação do Windows). Elas podem ser diferentes das listadas na coluna Volume de origem. No entanto, os dados serão restaurados no volume apropriado, mesmo quando as letras forem diferentes.

19. Após verificar se as informações de resumo estão corretas, clique em OK.

    O processo de restauração é iniciado. A tela do assistente de BMR exibe o status da restauração para cada volume.

    - Dependendo do tamanho do volume sendo restaurado, essa operação pode levar algum tempo.
    - Durante este processo, você estará restaurando bloco por bloco tudo o que tiver sido armazenado em backup para esse ponto de recuperação e criando uma réplica do computador de origem no computador de destino.
    - Por padrão, a opção que permite reiniciar o sistema automaticamente depois da recuperação é selecionada. Se necessário, você pode desmarcar esta opção e reinicializar manualmente mais tarde.
    - Se necessário, é possível cancelar ou anular a operação a qualquer momento.

20. No menu Utilitários, é possível acessar o Log de atividades da BMR e usar a opção Salvar para salvar o Log de atividades.

    Por padrão, o log de atividades será salvo no seguinte local:

    X:\windows\system32\dr\log.

    Observação: para evitar um erro gerado pelo Windows, não salve o Log de atividades na área de trabalho nem crie uma nova pasta na área de trabalho usando a opção Salvar como, na janela Log de atividades da BMR.

21. Caso esteja restaurando em diferentes tipos de hardware (o adaptador SCSI/FC usado para conectar unidades de disco rígido pode ter sido alterado) e nenhum driver compatível tenha sido detectado no sistema original, uma página de injeção de drivers será exibida para permitir o fornecimento de drivers a esses dispositivos.

    Procure e selecione os drivers a serem injetados no sistema recuperado de forma que, mesmo se estiver fazendo a recuperação em um computador com tipos diferentes de hardware, ainda seja possível trazer o computador de volta após a BMR.

22. Quando o processo de BMR for concluído, uma notificação de confirmação é exibida.

Observações: após a conclusão da BMR:

- O primeiro backup realizado é o Backup de verificação.
- Verifique se a BIOS está configurada para inicializar a partir do disco no qual o volume de inicialização foi restaurado.
- Após a reinicialização do computador, talvez seja necessário configurar os adaptadores de rede manualmente caso você tenha restaurado em um hardware diferente.
- Para discos dinâmicos, se o status do disco for offline, é possível alterá-lo manualmente para online na interface de gerenciamento de disco (acessado executando o utilitário de controle Diskmgmt.msc).
- Para discos dinâmicos, se os volumes dinâmicos estiverem em um status de falha de redundância, é possível sincronizar novamente os volumes na interface de gerenciamento de disco (acessado usando o utilitário de controle Diskmgmt.msc).

Recuperar servidores de origem usando dados de máquinas virtuais em modo de espera virtual no VMware

O aplicativo permite a recuperação de servidores de origem usando dados do CA ARCserve D2D que foram convertidos em máquinas virtuais em modo de espera virtual no VMware..

Observação: o aplicativo usa o processo de recuperação bare metal para recuperar servidores de origem máquinas virtuais do VMware. Para obter mais informações, consulte o tópico Recuperando servidores de origem usando uma recuperação bare metal (na página 116).

Para recuperar servidores de origem usando dados de máquinas virtuais em modo de espera virtual no VMware.

1. Insira a mídia da imagem do kit de inicialização salva e inicialize o computador.
   - Se estiver usando uma imagem salva do Windows PE, insira o CD/DVD da imagem do kit de inicialização.
   - Se estiver usando um dispositivo USB, insira o CD/DVD de instalação do Windows Server e conecte o dispositivo USB contendo a imagem salva do kit de inicialização.

   A tela do utilitário de instalação do BIOS é exibida.

2. Nessa tela, selecione a opção da unidade de CD-ROM para abrir o processo de inicialização.

   Observação: se estiver usando a imagem do Windows PE para executar uma BMR, selecione uma arquitetura (x86/x64) e pressione Enter para continuar.

3. A tela de seleção de idioma do CA ARCserve D2D é exibida. Selecione um idioma e clique em Avançar para continuar.

   Observação: se executar uma BMR com um USB e uma mídia de instalação do Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 (CD/DVD) sem suporte a MUI (Multilingual User Interface - Interface de Usuário Multilíngue), a tela de seleção de idioma não será exibida.

O processo de recuperação bare metal é iniciado, e a tela do assistente da BMR inicial é exibida.

4. Após selecionar a tela do assistente Selecionar o tipo de BMR (Bare Metal Recovery - Recuperação Bare Metal), selecione a opção Recuperar usando uma VM no modo de espera virtual do VMware.

BMR (Bare Metal Recovery - Recuperação Bare Metal) do CA ARCserve D2D
- Escolha um tipo de BMR

Especifique um tipo de recuperação:

○ **Recuperar dados cujo backup foi feito usando o CA ARCserve D2D**

(Sessões de backup usando o CA ARCserve D2D ou CA ARCserve Central Host-Based VM Backup).

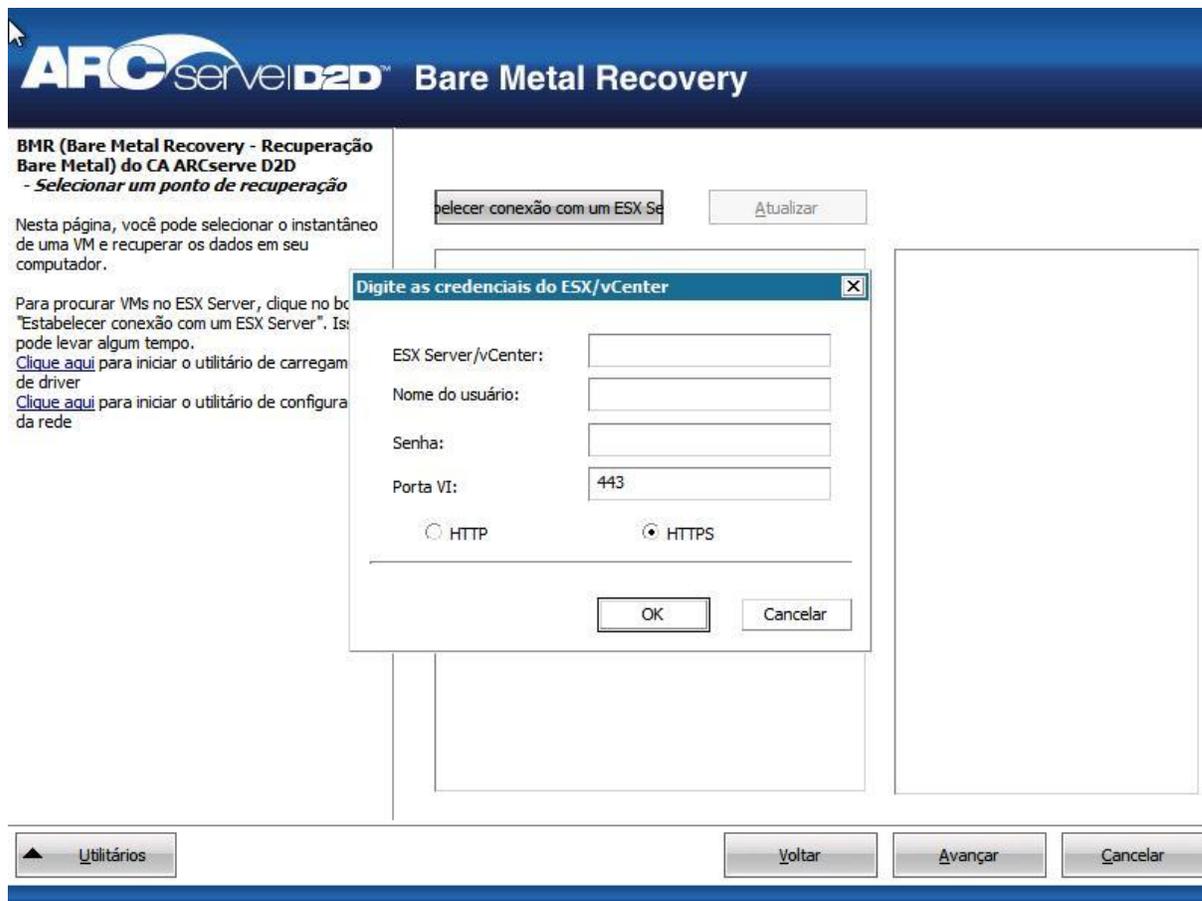
○ **Recuperar usando uma VM no modo de espera virtual do Hyper-V**

(é possível recuperar dados apenas se a conversão virtual tiver sido feita usando o CA ARCserve Central Virtual Standby)

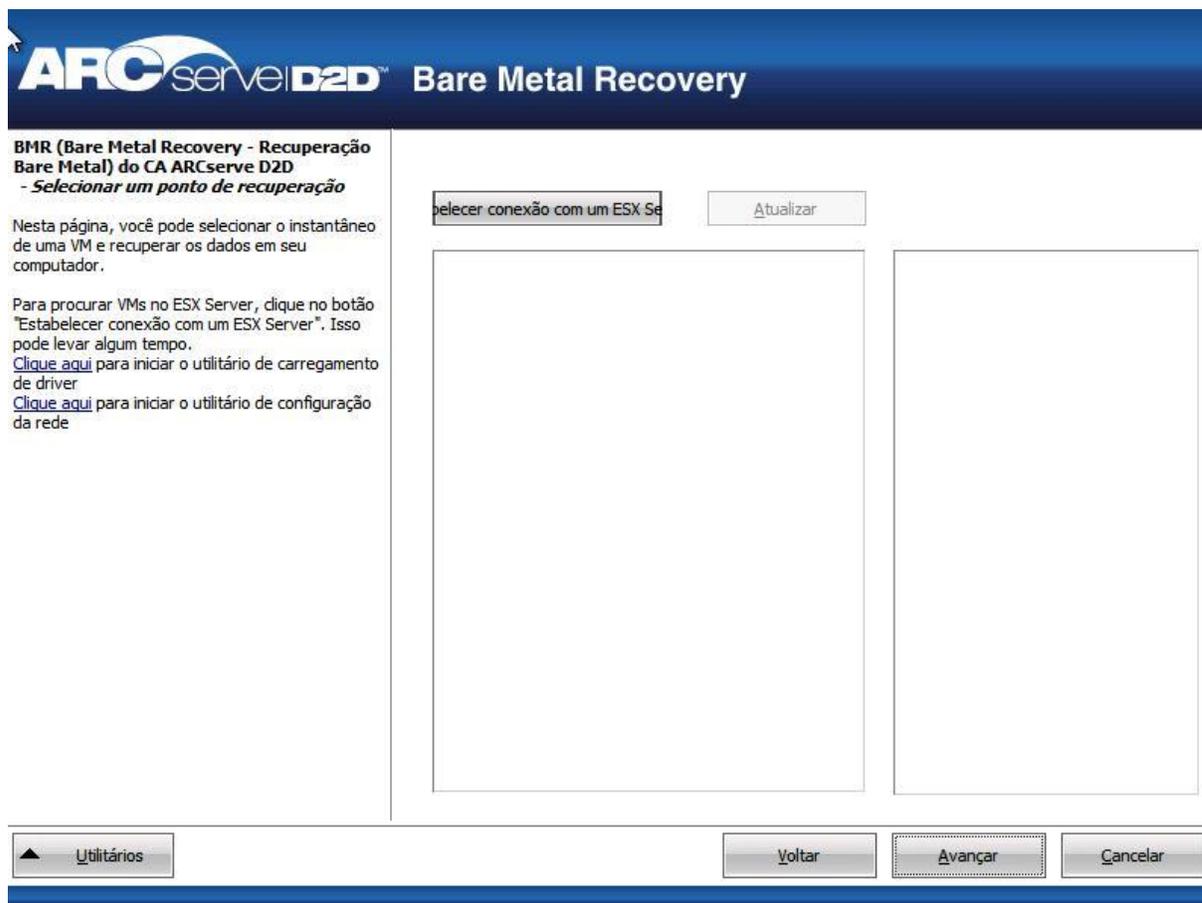
◉ **Recuperar usando uma VM no modo de espera virtual do VMware**

(é possível recuperar dados apenas se a conversão virtual tiver sido feita usando o CA ARCserve Central Virtual Standby)

5. Clique em Avançar.

   A tela Selecionar um ponto de recuperação é exibida com a caixa de diálogo Credenciais do ESX/VC.

6. Digite as informações da credencial, e clique em OK.

   A tela Selecionar um ponto de recuperação é exibida.

   Em seguida, o CA ARCserve D2D recupera todos os instantâneos do ponto de recuperação do servidor VMware selecionado e exibe o VMware Server no painel esquerdo com uma lista de todas as máquinas virtuais hospedadas no servidor VMware selecionado.

7. Selecione a máquina virtual que contenha pontos de recuperação da imagem de backup.

   As sessões de backup (instantâneos do ponto de recuperação) da máquina virtual selecionada são exibidas.

8. Selecione a sessão de backup da máquina virtual (instantâneos do ponto de recuperação) que deseja recuperar.

   Os detalhes correspondentes do instantâneo do ponto de recuperação selecionado (nome da máquina virtual, nome da sessão de backup, volumes armazenados em backup, discos dinâmicos com backup realizado) são exibidos no painel direito.

   Além disso, para selecionar um dos pontos de recuperação relacionados, tem-se a opção de selecionar o ponto de recuperação do estado atual ou do estado mais recente.

   - Se a máquina virtual que estiver recuperando estiver ligada, o ponto de recuperação do estado atual é exibido.
   - Se a máquina virtual que estiver recuperando estiver desligada, o ponto de recuperação do estado mais recente é exibido.

     Se selecionar o ponto de recuperação no estado mais recente, uma mensagem de erro será exibida para informar que o ponto de recuperação que você está recuperando é o estado mais recente (e não o atual) e solicitando que se inicie a máquina virtual antes de continuar com o processo de recuperação.

9. Verifique se este é o ponto de recuperação que deseja restaurar e clique em Avançar.

   Uma tela do assistente de BMR é exibida com as opções disponíveis do modo de recuperação.

10. Selecione o modo de recuperação.

    As opções disponíveis são Modo avançado e Modo expresso.

    - Selecione o Modo avançado, caso deseje personalizar o processo de recuperação.
    - Selecione o Modo expresso, se desejar o mínimo de interação durante o processo de recuperação.

    Padrão: Modo expresso.

    Observação: o restante desse procedimento é aplicável apenas se o modo avançado for selecionado e se o procedimento fornecer informações para orientá-lo durante o processo da BMR.

11. Clique em Avançar.

    O utilitário BMR inicia localizando o computador a ser recuperado e exibe as informações da partição de disco correspondente.

    O painel superior mostra a configuração de disco que você possui no computador atual (destino) e o painel inferior mostra as informações da partição de disco que havia no computador original (origem).

Importante: Um ícone vermelho em forma de X exibido para um volume de origem no painel inferior indica que o volume contém informações do sistema e não foi atribuído (mapeado) ao volume de destino. O volume contendo informações do sistema do disco de origem deve ser atribuído ao disco de destino e restaurado durante a BMR, caso contrário, haverá falha na reinicialização.

Observação: se executar a BMR e restaurar o volume do sistema em um disco que não está configurado como disco de inicialização, haverá falha ao iniciar o computador após o término da BMR. Verifique se está restaurando o volume do sistema em um disco de inicialização configurado corretamente.

Observação: ao restaurar em outro disco/volume, a capacidade do novo disco/volume deve ser do mesmo tamanho ou maior do que o disco/volume original. Além disso, o redimensionamento do disco destina-se somente a discos básicos, não a discos dinâmicos.

12. Se as informações do disco atual que você estiver vendo não parecem corretas, acesse o menu Utilitários e verifique se há drivers ausentes.

13. Se necessário, no painel de volume do destino, clique no menu suspenso Operações para exibir as opções disponíveis.

    Nesse menu, é possível redefinir as partições existentes ou criar partições que correspondam às partições de disco no volume de origem. (Redefinir significa recarregar as informações de layout do disco de origem e de destino a partir do arquivo de configuração e do sistema operacional atual, e descartar quaisquer informações de layout de disco alteradas pelo usuário).

    Observação: ao fazer mapeamento para outro disco, a capacidade de cada volume de destino mapeado deve ser do mesmo tamanho ou maior do que o volume de origem correspondente.

14. Clique em cada volume de destino e, no menu pop-up, selecione a opção Mapear volume de para atribuir um volume de origem a este volume de destino.

    A caixa de diálogo Selecionar um volume de origem básico é exibida.

15. Nesta caixa, clique no menu suspenso e selecione o volume de origem disponível para atribuí-lo ao volume de destino selecionado. Clique em OK.

    - No volume de destino, um ícone de marca de seleção é exibido, indicando que o volume de destino foi mapeado.
    - No volume de origem, o ícone em forma de X vermelho muda para verde, indicando que o volume de origem foi atribuído a um volume de destino.

16. Quando tiver certeza de que todos os volumes que desejar restaurar e todos os volumes que tiverem informações do sistema foram atribuídos a um volume de destino, clique em Avançar.

    A tela Enviar alterações de disco é exibida, mostrando um resumo das operações selecionadas. Para cada novo volume criado, são exibidas as informações correspondentes.

17. Ao confirmar se as informações de resumo estão corretas, clique em Enviar. (Se não estiverem corretas, clique em Cancelar.)

    Observação: as operações no disco rígido não entrarão em vigor até que sejam enviadas.

    No computador de destino, os novos volumes são criados e mapeados para o computador de origem correspondente.

18. Quando as alterações forem concluídas, clique em OK.

    A tela Resumo das configurações de restauração é exibida, mostrando um resumo dos volumes a serem restaurados.

    Observação: na parte inferior da janela de resumo da restauração, as letras de unidade listadas na coluna Volume de destino são geradas automaticamente no WinPE (Windows Preinstallation Environment - Ambiente de Pré-Instalação do Windows). Elas podem ser diferentes das listadas na coluna Volume de origem. No entanto, os dados serão restaurados no volume apropriado, mesmo quando as letras forem diferentes.

19. Após verificar se as informações de resumo estão corretas, clique em OK.

    O processo de restauração é iniciado. A tela do assistente de BMR exibe o status da restauração para cada volume.

    - Dependendo do tamanho do volume sendo restaurado, essa operação pode levar algum tempo.
    - Durante este processo, você estará restaurando bloco por bloco tudo o que tiver sido armazenado em backup para esse ponto de recuperação e criando uma réplica do computador de origem no computador de destino.
    - Por padrão, a opção que permite reiniciar o sistema automaticamente depois da recuperação é selecionada. Se necessário, você pode desmarcar esta opção e reinicializar manualmente mais tarde.
    - Se necessário, é possível cancelar ou anular a operação a qualquer momento.

20. No menu Utilitários, é possível acessar o Log de atividades da BMR e usar a opção Salvar para salvar o Log de atividades.

    Por padrão, o log de atividades será salvo no seguinte local:

    X:\windows\system32\dr\log.

    Observação: para evitar um erro gerado pelo Windows, não salve o Log de atividades na área de trabalho nem crie uma nova pasta na área de trabalho usando a opção Salvar como, na janela Log de atividades da BMR.

21. Caso esteja restaurando em diferentes tipos de hardware (o adaptador SCSI/FC usado para conectar unidades de disco rígido pode ter sido alterado) e nenhum driver compatível tenha sido detectado no sistema original, uma página de injeção de drivers será exibida para permitir o fornecimento de drivers a esses dispositivos.

    Procure e selecione os drivers a serem injetados no sistema recuperado de forma que, mesmo se estiver fazendo a recuperação em um computador com tipos diferentes de hardware, ainda seja possível trazer o computador de volta após a BMR.

22. Quando o processo de BMR for concluído, uma notificação de confirmação é exibida.

Observações: após a conclusão da BMR:

- O primeiro backup realizado é o Backup de verificação.
- Verifique se a BIOS está configurada para inicializar a partir do disco no qual o volume de inicialização foi restaurado.
- Após a reinicialização do computador, talvez seja necessário configurar os adaptadores de rede manualmente caso você tenha restaurado em um hardware diferente.
- Para discos dinâmicos, se o status do disco for offline, é possível alterá-lo manualmente para online na interface de gerenciamento de disco (acessado executando o utilitário de controle Diskmgmt.msc).
- Para discos dinâmicos, se os volumes dinâmicos estiverem em um status de falha de redundância, é possível sincronizar novamente os volumes na interface de gerenciamento de disco (acessado usando o utilitário de controle Diskmgmt.msc).

Restaurar mensagens de email do Microsoft Exchange

O Virtual Standby permite restaurar dados do Microsoft Exchange a partir de pontos de recuperação do CA ARCserve D2D. A partir dos pontos de recuperação, você pode recuperar ou restaurar caixas de correio, pastas e mensagens de email individuais.

Observação: para executar restaurações granulares de dados do Exchange Server, sua conta deve ter as permissões de acesso necessárias. Para obter mais informações, consulte o *Guia do Usuário do CA ARCserve D2D*.

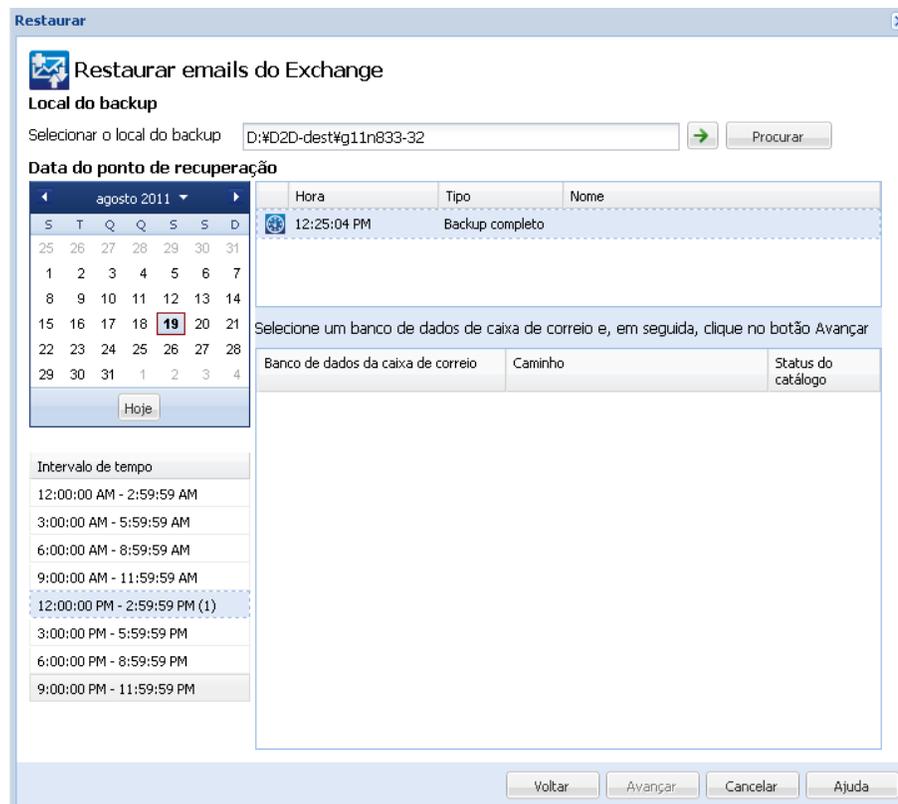
Para restaurar mensagens de email do Microsoft Exchange

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

2. Na caixa de diálogo Restaurar, clique em Restaurar emails do Exchange.

   A caixa de diálogo Restaurar emails do Exchange é aberta.

3. Especificar o local do backup. Você pode especificar um local ou procurar o local onde as suas imagens de backup estão armazenadas. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local. Pode-se clicar no ícone de validação em forma de seta verde para confirmar o devido acesso ao local de origem.

   A exibição do calendário realçará (em verde) todas as datas do período exibido que contiverem os pontos de recuperação para essa origem de backup.

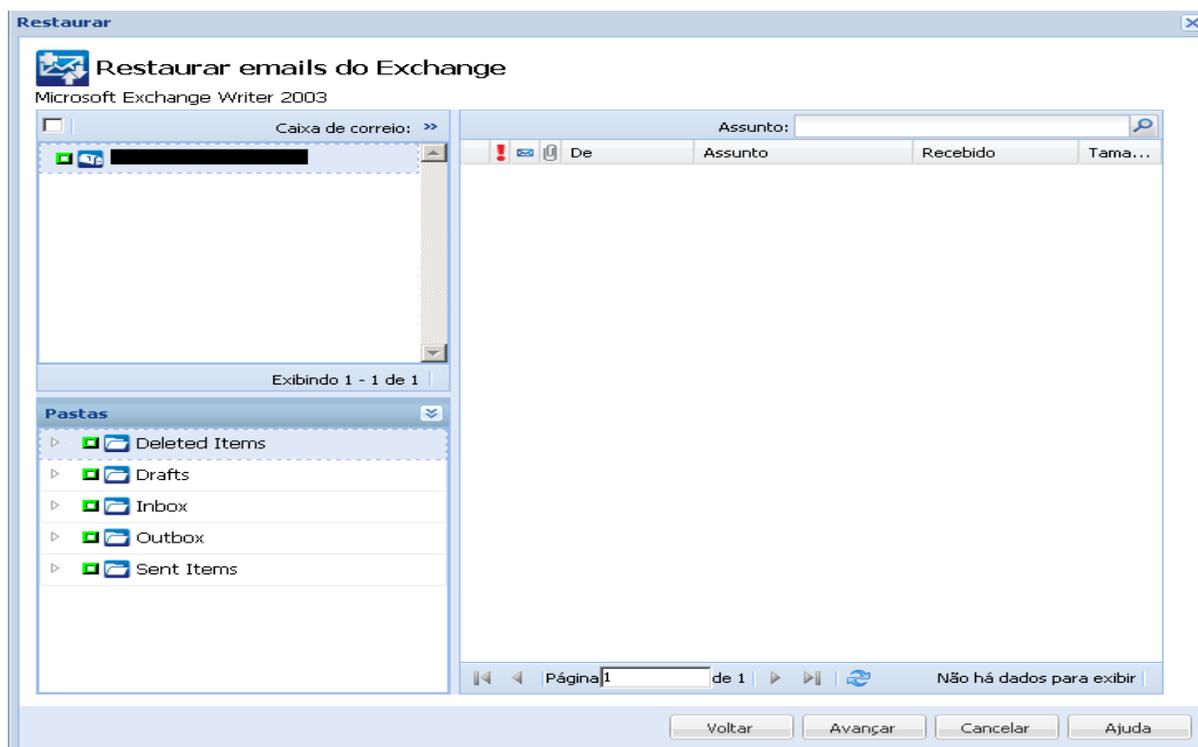
4. Selecione a data no calendário para a imagem de backup que deseja restaurar.

   Os bancos de dados da caixa de correio do Exchange correspondentes a essa data são exibidos juntamente com a hora do backup, o tipo de backup que foi executado e o nome do backup.

5. Selecione um banco de dados da caixa de correio do Exchange que deseja restaurar e clique em Avançar.

   Observação: se não ativar a opção Restauração granular do Exchange durante o backup (nenhum catálogo gerado), uma mensagem de notificação será exibida perguntando se deseja gerar um catálogo da restauração granular do Exchange naquele momento. Caso selecione Não gerar um catálogo agora, não será possível procurar ou selecionar um ponto de recuperação granular. Como resultado, só será possível executar a restauração total do banco de dados a partir da caixa de diálogo Procurar pontos de recuperação para restaurar.

A caixa de diálogo Restaurar emails do Exchange é atualizada para exibir uma lista do conteúdo da caixa de correio do banco de dados selecionado.

Observação: a restauração granular do Exchange oferece suporte apenas a email. As restaurações de calendário, contatos, observações e tarefas não são suportadas.

6. Selecione o nível de objeto(s) do Exchange a ser(em) restaurado(s) (caixa de correio, pasta ou email individual).

   É possível selecionar parte ou todo o conteúdo do objeto do Exchange a ser restaurado. Você pode selecionar vários objetos do Exchange a serem restaurados.

   Observação: o CA ARCserve D2D não oferece suporte à recuperação granular de objetos da pasta pública do Exchange. Você precisa usar a restauração de aplicativo para recuperar todo o banco de dados da pasta pública e, em seguida, extrair o objeto do Exchange desejado.

   Observação: ao usar o CA ARCserve D2D para restaurar objetos da caixa de correio/email individuais a partir do banco de dados da caixa de correio do Exchange, o sistema operacional usado para a restauração deve ser o mesmo usado no backup (incluindo o mesmo número de versão e nível de Service Pack do Windows, bem como a versão relacionada do pacote redistribuível Visual C++ necessário para suportá-lo).

Observação: ao procurar e restaurar emails da interface do usuário do CA ARCserve D2D, é possível que a propriedade do campo "De" da mensagem não seja exibida na interface do usuário para as caixas de correio que nunca se conectaram ao servidor do Exchange. Se isso ocorrer, os emails ainda serão restaurados corretamente.

a. É possível selecionar um banco de dados da caixa de correio.

   Se selecionar um banco de dados da caixa de correio, todas as caixas de correio naquele banco de dados serão restauradas.

b. Pode-se selecionar a caixa de correio (ou caixas de correio) a ser restaurada.

   Se selecionar um nível da caixa de correio, todo o conteúdo correspondente (pastas e emails individuais) daquela caixa de correio será restaurado.

c. É possível selecionar uma ou mais pastas de uma caixa de correio selecionada para ser(em) restaurada(s).

   Se você selecionar o nível de pasta da caixa de correio, todo o conteúdo de email correspondente daquela pasta será restaurado.

d. Você pode selecionar os emails individuais a serem restaurados.

   Se selecionar o nível de email individuais, apenas o(s) objeto(s) de email selecionado(s) será(ão) restaurado(s).

   Observação: apenas para o Exchange 2003, se o email individual a ser restaurado foi enviado usando qualquer cliente de email diferente do Outlook e, se durante o backup, havia no email algum tipo de marcador de status do sinalizador anexado, o email será restaurado, mas o marcador anexo não será incluído nele.

7. Quando os objetos do Exchange a serem restaurados forem especificados, clique em Avançar.

Restaurar

Opções de restauração

Destino

Selecionar o destino da restauração.

Restaurar no local original

Nome de usuário G11N32¥Administrator

Senha •••

Itens de email de despejo Procurar

Como o CA ARCserve D2D deve resolver emails duplicados

Renomear Substituir

Restaurar em um local diferente

Insira a conta e clique no botão Procurar para escolher o destino.

Nome de usuário G11N32¥Administrator

Senha •••

Destino Procurar

Observações:

Para os sistemas Exchange Server 2003, o nome de usuário deve ser de uma conta de domínio com a função completa de administrador do Exchange.

Voltar Avançar Cancelar Ajuda

8. Selecione o destino da restauração.

As opções disponíveis são restaurar no local original do backup ou restaurar em um local diferente.

Observação: para o Exchange 2010, os itens arquivados da caixa de correio podem ser restaurados no local original. Os itens arquivados da caixa de correio só podem ser restaurados em um local diferente ou em um disco local. Além disso, os itens regulares da caixa de correio não podem ser restaurados em caixas de correio arquivadas.

Restaurar no local original

Restaura os emails no local original a partir do qual a imagem de backup foi capturada. Os emails manterão a mesma hierarquia e serão restaurados em sua pasta e caixa de correio originais.

- Se o computador atual não for o servidor ativo do Exchange, o CA ARCserve D2D detectará o local do servidor ativo e tentará restaurar os emails naquele servidor.
- Se a caixa de correio foi movida para outro servidor do Exchange, mas ainda estiver na mesma organização, o CA ARCserve D2D detectará o novo servidor do Exchange em que a caixa de correio original reside, e fará a restauração neste servidor.
- Se o nome de exibição da caixa de correio foi alterado, qualquer tentativa de restaurá-la (a partir de uma sessão de backup anterior) em seu local original irá falhar, pois o CA ARCserve D2D não conseguirá localizar o nome alterado. Para resolver esse problema, é possível especificar restaurar esta caixa de correio em um local diferente.

Observação: ao restaurar uma caixa de correio ou email no local original, certifique-se de que a caixa de correio de destino esteja disponível, caso contrário, haverá falha na restauração. O CA ARCserve D2D apenas valida o destino quando a tarefa de restauração é enviada.

Apenas arquivo de despejo

Restaura os emails em um disco. O local do disco pode ser máquina local ou remota. Os emails restaurados manterão a mesma hierarquia que tinham na caixa de correio do Exchange correspondente. O nome do arquivo será o assunto do email.

Observação: se o assunto do email, nome da pasta ou nome da caixa de correio incluir os seguintes caracteres, o caractere será substituído por hífen (-) no nome do arquivo: \ / : * ? " < > |

Para esta opção, é necessário também especificar o que deseja que o CA ARCserve D2D faça para resolver uma situação de conflito. No Exchange, pode-se ter vários objetos de email com o mesmo nome na mesma pasta. No entanto, em um sistema de arquivos, dois arquivos com o mesmo nome não podem coexistir na mesma pasta.

Há duas opções para resolver essa situação de conflito:

- **Renomear** - se no disco houver um arquivo com o mesmo nome do assunto de email, o CA ARCserve D2D ainda nomeará o assunto do email, mas acrescentará um número no final.
- **Substituir** - se no disco houver um arquivo com o mesmo nome do assunto de email, o CA ARCserve D2D substituirá esse arquivo.

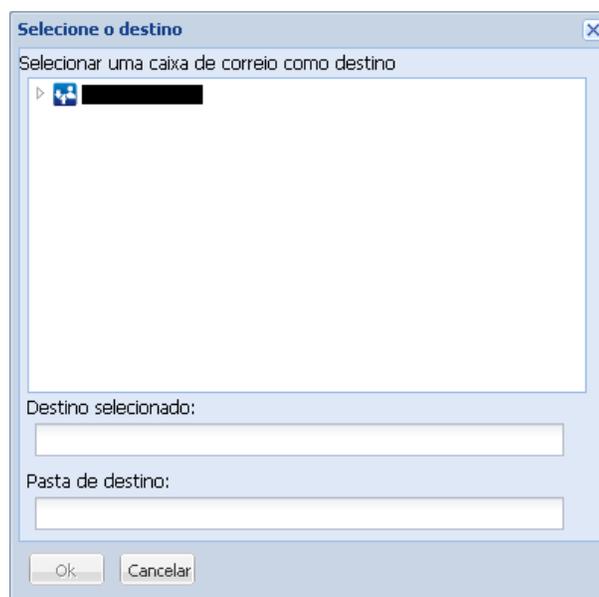
Observação: ao selecionar objetos de email individuais para restaurar no disco (despejo), por padrão, o formato do objeto de email restaurado será um arquivo de mensagem do Outlook (.MSG), e não um arquivo de tabela de armazenamento pessoal (.PST).

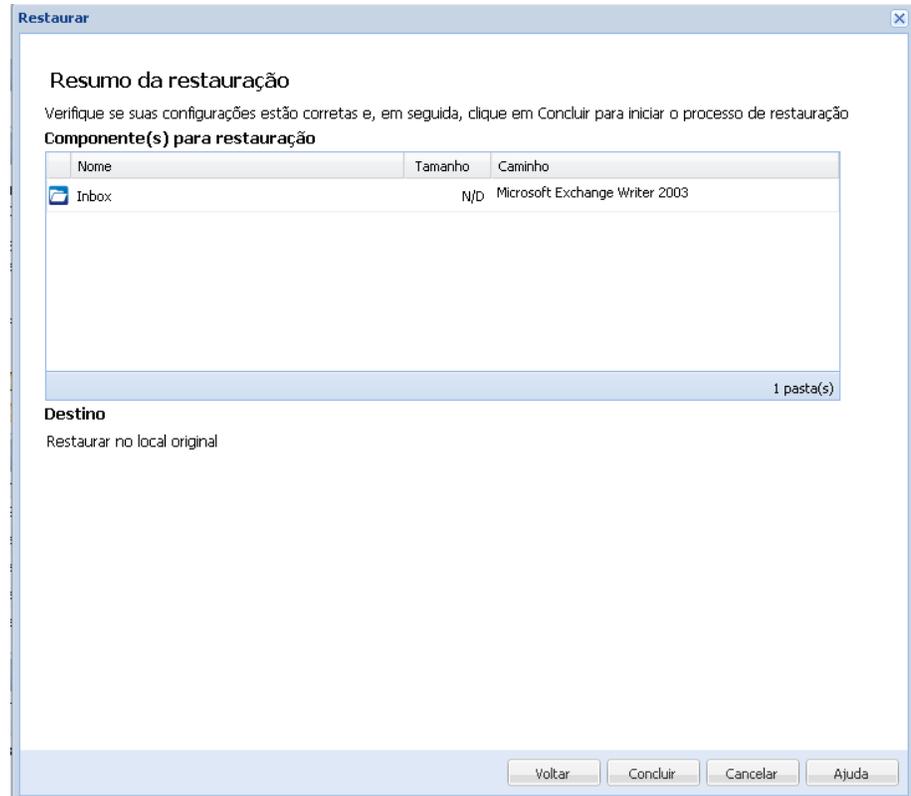
Restaurar em um local diferente:

Restaura os emails em um local especificado ou permite procurar o local onde as imagens de backup serão restauradas. O destino deve ser uma caixa de correio na mesma organização do Exchange, e um novo nome da pasta é necessário. (Se estiver tentando restaurar emails em um local diferente, o destino não pode ser uma pasta pública.)

Observação: ao restaurar email em um local alternativo, se a pasta de destino especificada já existir, a restauração continuará. No entanto, se a pasta especificada não existir, então CA ARCserve D2D irá criar a pasta primeiro e, em seguida, continuar a restauração.

Após inserir o nome de usuário e a senha, é possível clicar no botão Procurar para navegar por uma lista de todos os servidores do Exchange, grupos de armazenamento, bancos de dados do Exchange e caixas de correio na organização atual.

Selecione a caixa de correio como o destino.

9. Quando as opções de restauração forem selecionadas, clique em Avançar.

   A caixa de diálogo Resumo da restauração é exibida.

10. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

    - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.
    - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

    Observação: quando a tarefa de restauração e de geração de catálogo da restauração granular do Exchange estiver em andamento, a sessão de backup estará em um estado montado. Não executar nenhuma operação (formato, alterar letra de unidade, excluir partição, etc.) no volume montado.

Alterar o protocolo de comunicação do servidor

Por padrão, o CA ARCserve Central Applications usa o protocolo HTTP (Hypertext Transfer Protocol) para comunicação entre todos os seus componentes. Caso esteja preocupado com a segurança das senhas comunicadas entre esses componentes, é possível alterar o protocolo em uso para HTTPS (Hypertext Transfer Protocol Secure). Além disso, se você não precisar deste nível extra de segurança, é possível alterar o protocolo em uso para HTTP.

Siga estas etapas:

1. Efetue logon no computador no qual o aplicativo está instalado usando uma conta administrativa ou uma conta com privilégios administrativos.

   Observação: se não efetuar logon usando uma conta administrativa ou uma conta com privilégios administrativos, configure a linha de comando para ser executada usando o privilégio Run as Administrator.

2. Abra a linha de comando do Windows.

3. Siga um destes procedimentos:

   - **Para alterar o protocolo de HTTP para HTTPS:**

     Inicie a ferramenta de utilitário changeToHttps.bat no seguinte local padrão (o local da pasta BIN pode variar dependendo de onde você instalou o aplicativo):

     ```
     C:\Arquivos de Programas\CA\ARCserve Central Applications\BIN
     ```

     Quando o protocolo for alterado com êxito, a seguinte mensagem será exibida:

     ```
     O protocolo de comunicação foi alterado para HTTPS.
     ```

   - **Para alterar o protocolo de HTTPS para HTTP:**

     Inicie a ferramenta de utilitário changeToHttp.bat no seguinte local padrão (o local da pasta BIN pode variar dependendo de onde você instalou o aplicativo):

     ```
     C:\Arquivos de Programas\CA\ARCserve Central Applications\BIN
     ```

     Quando o protocolo for alterado com êxito, a seguinte mensagem será exibida:

     ```
     O protocolo de comunicação foi alterado para HTTP.
     ```

4. Reinicie o navegador e reconecte-se ao CA ARCserve Central Applications.

   Observação: quando você altera o protocolo para HTTPS, um aviso é exibido no navegador web. Esse comportamento ocorre devido a um certificado de segurança autoassinado que solicita que você ignore o aviso e continue ou adicione esse certificado ao navegador para evitar que o aviso seja exibido novamente.

Capítulo 5: Solucionando problemas do CA ARCserve Central Virtual Standby

Esta seção fornece informações sobre solução de problemas para ajudá-lo a identificar e resolver problemas que possam ocorrer durante o uso do CA ARCserve Central Virtual Standby.

Esta seção contém os seguintes tópicos:

Não é possível se conectar ao servidor especificado, mensagens são exibidas ao tentar adicionar nós

Válido em plataformas Windows.

Sintoma:

A mensagem a seguir é exibida ao tentar adicionar ou se conectar a nós na tela Nó.

`Não é possível se conectar ao servidor especificado.`

Solução:

Se a mensagem acima for exibida ao tentar adicionar nós a partir da tela Nó, as seguintes ações corretivas podem ajudar a resolver o problema:

- Verifique se o serviço do Windows Server está em execução na máquina virtual de origem (nó) e no servidor do CA ARCserve Central Virtual Standby.
- Verifique se uma exceção do Windows Firewall foi aplicada ao serviço de compartilhamento de arquivo e impressora do Windows na máquina virtual de origem (nó) e no servidor do CA ARCserve Central Virtual Standby.
- Verifique se uma exceção do Windows Firewall foi aplicada ao serviço Netlogon do Windows apenas se o nó não for integrante de um domínio. Execute esta tarefa na máquina virtual de origem (nó) e no servidor do CA ARCserve Central Virtual Standby.
- Verifique se o valor aplicado ao modelo de compartilhamento e segurança para contas locais é Clássico. Para aplicar o valor Clássico proceda da seguinte maneira:

  Observação: execute as etapas a seguir na máquina virtual de origem (nó) e no servidor do CA ARCserve Central Virtual Standby.

  1. Efetue logon no servidor do CA ARCserve Central Virtual Standby e abra o painel de controle.
  2. No Painel de controle, abra Administrative Tools.
  3. Clique duas vezes em Diretiva de segurança local.

     A janela Diretiva de segurança local é exibida.

4. Nesta janela, expanda Diretivas locais e expanda Opções de segurança.

   As diretivas de segurança são exibidas.

5. Clique com o botão direito do mouse em Network access: Sharing and security model for local accounts e clique em Propriedades no menu pop-up.

   A caixa de diálogo Network access: Sharing and security model for local accounts properties é exibida.

6. Clique em Configuração de segurança local.

   Na lista suspensa, selecione Clássico - os usuários locais são autenticados como eles mesmos.

   Clique em OK.

- Verifique se o valor aplicado às Diretivas locais para o nível de autenticação do LAN Manager é definido para enviar LM & NTLMv2 - usar a segurança da sessão NTLMv2, se negociado. Para aplicar o valor, proceda da seguinte maneira:

  1. Efetue logon no servidor do CA ARCserve Central Virtual Standby e abra o prompt de comando.

     Execute o seguinte comando

     ```
     secpol.msc
     ```

     A caixa de diálogo Configurações de Segurança Local é exibida.

  2. Selecione as diretivas locais e clique em opções de segurança.

     Pesquise a segurança de rede: nível de autenticação do LAN Manager.

     Clique duas vezes na opção.

     A caixa de diálogo Propriedades é aberta

  3. Selecione a opção a seguir e clique em OK.

     ```
     enviar LM & NTLMv2 - usar a segurança da sessão NTLMv2, se negociado
     ```

  4. No prompt de comando, execute o seguinte:

     ```
     gpupdate
     ```

  O valor é aplicado.

Páginas da web em branco são exibidas ou ocorrem erros no Javascript

Válido para os sistemas operacionais Windows Server 2008 e Windows Server 2003.

Sintoma:

Ao abrir os sites da web do CA ARCserve Central Applications usando o Internet Explorer, páginas da web em branco são exibidas ou ocorrem erros no Javascript. O problema ocorre ao abrir o Internet Explorer em sistemas operacionais Windows Server 2008 e Windows Server 2003.

Esse problema ocorre nas seguintes condições:

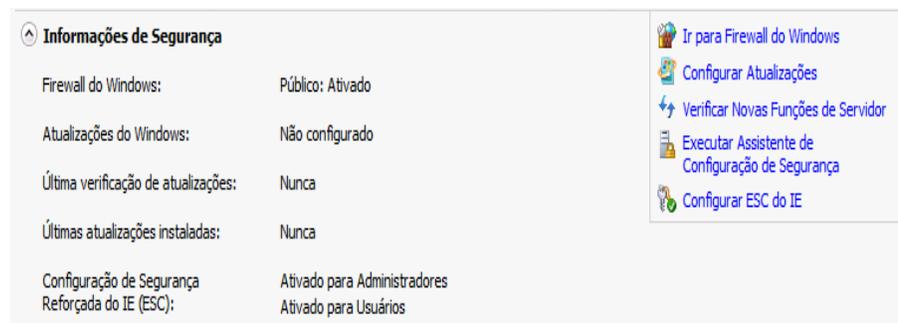
- Você está usando o Internet Explorer 8 ou Internet Explorer 9 para exibir o aplicativo e o navegador não reconhece o URL como um site confiável.
- Você está usando o Internet Explorer 9 para exibir o aplicativo e o protocolo de comunicação em uso é HTTPS.

Solução:

Para corrigir este problema, desative a opção Segurança aprimorada do Internet Explorer nos computadores usados para exibir o aplicativo.

Para desativar esta opção em sistemas Windows Server 2008, faça o seguinte:

1. Faça logon no computador com Windows Server 2008 que você usa para exibir os relatórios usando a conta de administrador ou uma conta que tenha privilégios administrativos.
2. Clique com o botão direito do mouse em Computador na área de trabalho e clique em Gerenciar para abrir a janela Gerenciador do servidor.
3. Na janela Gerenciador do servidor, clique em Gerenciador do servidor (nome do servidor).

   Na seção Server Summary, abra Security Information e clique em Configure IE ESC, conforme ilustrado abaixo:

   A caixa de diálogo Enhanced Security Configuration do Internet Explorer é aberta.

4. Neste caixa de diálogo, faça o seguinte:
   - Administrators--Click Desativado
   - Usuários--Clique em Desativar.

   Clique em OK.

A caixa de diálogo Internet Explorer Enhanced Security Configuration é fechada e segurança reforçada do Internet Explorer é desativada.

Para desativar esta opção em sistemas Windows Server 2003, faça o seguinte:

1. Faça logon no computador com Windows Server 2003 que você usa para exibir os relatórios usando a conta de administrador ou uma conta que tenha privilégios administrativos.
2. Abra o Painel de Controle do Windows e, em seguida, abra Add or Remove Programs.
3. Na caixa de diálogo Add or Remove Programs, clique na opção Add/Remove Windows Components para acessar a tela Windows Components Wizard.

   Desmarque a caixa de seleção próxima a Configuração de segurança aprimorada do Internet Explorer.

   Clique em Avançar.

   Siga as instruções na tela para concluir a instalação e clique em Concluir.

A opção Internet Explorer Enhanced Security é desativada.

Resolução de problemas do carregamento da página

Válido em plataformas Windows.

Sintoma:

As seguintes mensagens de erro podem ser exibidas em janelas de navegador ao efetuar logon em nós do CA ARCserve Central Applications, CA ARCserve D2D e servidores de monitoramento.

Mensagem 1:

```
Os erros nesta página podem fazer com que ela funcione incorretamente.
```

Mensagem 2:

```
!
```

Solução:

As páginas da web podem não ser carregadas corretamente por vários motivos. A tabela a seguir descreve os motivos comuns e as respectivas ações corretivas:

Razão	Ação corretiva
Há problemas com o código fonte HTML subjacente.	Atualize a página da web e tente novamente.
Sua rede bloqueia o Script ativo, ActiveX, ou os programas Java.	Permita que seu navegador use Script ativo, ActiveX ou programas Java.
Seu aplicativo antivírus está configurado para examinar arquivos temporários da Internet e programas cujo download foi concluído.	Filtre o aplicativo antivírus para permitir arquivos relacionados à Internet associados a páginas da web do CA ARCserve Central Applications.
O mecanismo de script instalado em seu computador está corrompido ou desatualizado.	Atualize o mecanismo de script.
A placa de vídeo instaladas no computador estão corrompidas ou desatualizadas.	Atualize-as.
O componente DirectX instalado em seu computador está corrompido ou desatualizado.	Atualize-o.

Páginas da web não são carregadas adequadamente ao efetuar logon em nós e servidores de monitoramento do CA ARCserve D2D.

Válido em plataformas Windows.

Sintoma:

As páginas da web nas janelas do navegador não são carregadas corretamente, exibem mensagens de erro, ou ambos ao efetuar logon em nós e servidores de monitoramento do CA ARCserve D2D na tela Nós.

Solução:

Esse comportamento afeta principalmente os navegadores Internet Explorer. As páginas da web podem não ser carregadas corretamente quando scripts ativos, controles ActiveX ou programas Java estiverem desativados no computador ou bloqueados na rede.

É possível corrigir o problema com a atualização da janela do navegador. No entanto, se a atualização do navegador não corrigir o problema, faça o seguinte:

1. Abra o Internet Explorer.

   No menu Ferramentas, clique em Opções da Internet.

   A caixa de diálogo Opções da Internet é aberta.

2. Clique na guia Segurança.

   As opções de segurança são exibidas:

3. Clique em Zona da Internet.

   As opções de zona da Internet são exibidas.

4. Clique em Nível personalizado.

   A caixa de diálogo Security Settings - Internet Zone é aberta.

5. Rolar para a categoria Script.

   Localize o Script ativo.

   Clique na opção Ativar ou Solicitar.

6. Clique em OK na caixa de diálogo Security Settings - Internet Zone.

   A caixa de diálogo Security Settings - Internet Zone é fechada.

7. Clique em OK na caixa de diálogo Internet Options.

   Esta caixa de diálogo é fechada e a opção Script ativo é aplicada.

Observação: se esta solução não corrigir o problema, consulte o administrador do sistema para verificar se os outros programas, como programas antivírus ou de firewall, não estão bloqueando os scripts ativos, os controles ActiveX ou os programas do Java.

Caracteres sem sentido são exibidos no navegador do Windows ao acessar o CA ARCserve Central Applications

Válido em todos os sistemas operacionais Windows. Todos os navegadores afetados.

Sintoma:

Ao efetua logon no CA ARCserve Central Applications, caracteres sem sentido aparecem na área de conteúdo da janela do navegador.

Solução:

Este problema ocorre ao instalar o CA ARCserve Central Applications usando a comunicação HTTPS e ao tentar acessar o CA ARCserve Central Applications usando a comunicação HTTP. O componente subjacente dos serviços web do CA ARCserve Central Applications não oferece suporte ao recurso para converter URLs HTTP para URLs HTTPS. Como resultado, os caracteres sem sentido aparecem na janela do navegador. Por exemplo:

Para corrigir esse problema, acesse o CA ARCserve Central Applications usando o HTTPS ao instalar ou configurar aplicativos para se comunicar usando o HTTPS.

Falha de serviço web do CA ARCserve D2D em nós do CA ARCserve D2D

Válido em plataformas Windows.

Sintoma:

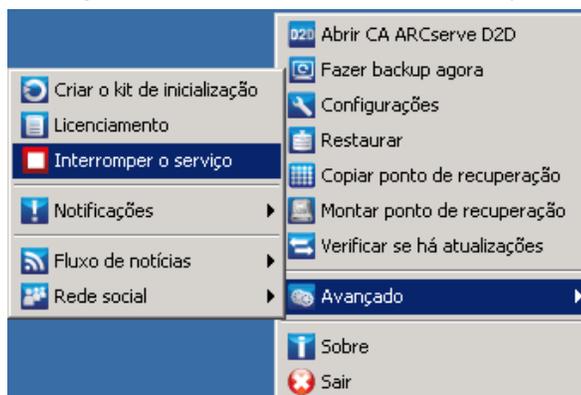
O serviço web em execução em nós do CA ARCserve D2D é iniciado e falha ou não pode ser iniciado.

Solução:

Esse problema ocorre quando a porta usada pelo serviço web do CA ARCserve D2D é a mesma que a porta usada pelo serviço web do VMware vCenter (Tomcat).

A porta usada pelo CA ARCserve D2D pode entrar em conflito com a porta padrão usada pelo Tomcat. Esse conflito gera falha no Tomcat quando o CA ARCserve D2D é iniciado antes dele. Para corrigir este problema, pode-se alterar a porta padrão do Tomcat, como segue:

1. Acesse o monitor do CA ARCserve D2D, clique na opção Avançado e selecione Interromper o serviço.

   O serviço web do CA ARCserve D2D é interrompido.

2. Acesse o arquivo server.xml para editar/configurar o comportamento do Tomcat.

   O arquivo server.xml está localizado na seguinte estrutura de pastas:

   ```
   C:\Arquivos de programas\CA\ARCserve Central Applications\TOMCAT\conf
   ```

3. Localize a marca <Server> no arquivo server.xml.

```
      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or impli
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<!-- Note:  A "Server" is not itself a "Container", so you may not
     define subcomponents such as "Valves" at this level.
     Documentation at /docs/config/server.html
 -->
<Server>
        <!--APR library loader. Documentation at /docs/apr.html -->
        <Listener className="org.apache.catalina.core.AprLifecycleListe
        <!--Initialize Jasper prior to webapps are loaded. Documentatio
        <Listener className="org.apache.catalina.core.JasperListener"/>
        <!-- JMX Support for the Tomcat server. Documentation at /docs/
        <Listener className="org.apache.catalina.mbeans.ServerLifecycle
        <Listener className="org.apache.catalina.mbeans.GlobalResources
        <!-- Global JNDI resources
       Documentation at /docs/jndi-resources-howto.html
  -->
        <GlobalNamingResources>
                <!-- Editable user database that can also be used by
```

4. Edite a marca <Server>, como segue:

   De:

   <Server>

   Para:

   <Server port="8015" shutdown="SHUTDOWN">

5. Salve e feche o arquivo server.xml.

   O comando para desligar o Tomcat agora foi configurado de forma que ele seja recebido pelo servidor na porta especificada (8015).

6. Acesse o monitor do CA ARCserve D2D, clique na opção Avançado e selecione Iniciar o serviço.

   O serviço web do CA ARCserve D2D é iniciado.

O serviço web do CA ARCserve D2Dé executado lentamente

Válido em sistemas operacionais Windows.

Sintoma 1:

O serviço web do CA ARCserve D2D em sistemas do CA ARCserve D2D é executado lentamente. É possível detectar outros sintomas, tais como:

- O serviço web do CA ARCserve D2D pára de responder ou ocupa 100% dos recursos da CPU.
- A comunicação dos nós do CA ARCserve D2D com o serviço web é insatisfatória ou não existe.

Solução 1:

Em diversas configurações de ambiente, é possível descobrir que o serviço web do CA ARCserve D2D ocupa muito tempo da CPU, ou a resposta é lenta. Por padrão, o Tomcat é configurado para alocar uma quantidade limitada de memória para os nós, que talvez não seja adequada para seu ambiente. Para verificar esse problema, revise os arquivos de log a seguir:

```
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log
```

Procure a seguinte mensagem:

```
java.lang.OutOfMemoryError
```

Para corrigir este problema, aumente a quantidade de memória alocada.

Para aumentar a memória, proceda da seguinte maneira:

1. Abra o Registry Editor e acesse a chave a seguir:
   - Sistemas operacionais x86:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java
     ```

   - Sistemas operacionais x64:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java
     ```

2. Siga um destes procedimentos:

   - Se a mensagem no arquivo de log for:

     ```
     java.lang.OutOfMemoryError: PermGen space
     ```

     Acrescente o seguinte valor de opções.

     ```
     -XX:PermSize=128M -XX:MaxPermSize=128M
     ```

     Observação: talvez seja necessário aumentar o valor de -XX:MaxPermSize de acordo com seu ambiente.

   - Se a mensagem no arquivo de log for:

     ```
     java.lang.OutOfMemoryError: Java heap space
     java.lang.OutOfMemoryError: GC overhead limit exceeded
     ```

     Aumente o valor de DWORD a seguir:

     ```
     JvmMx
     ```

3. Reinicie o serviço web do CA ARCserve D2D.

Sintoma 2

Os backups programados são ignorados e a execução é interrompida.

Solução 2

Ao configurar o valor MAX como 20 ou menos de 20 para backups simultâneos, faça o seguinte:

1. Aumente o valor de DWORD a seguir:

   ```
   JvmMx=256
   ```

   Observação: esse DWORD é mencionado na Solução 1.

2. Acrescente o seguinte valor de opções.

   ```
   -XX:MaxPermSize=128M
   ```

   Observação: esse DWORD é mencionado na Solução 1.

Ao configurar o valor MAX como mais de 20, mas menos que 50 para backups simultâneos, faça o seguinte:

1. Aumente o valor de DWORD a seguir:

   ```
   JvmMx=512
   ```

   Observação: esse DWORD é mencionado na Solução 1.

2. Acrescente o seguinte valor de opções.

   ```
   -XX:MaxPermSize=256M
   ```

   Observação: esse DWORD é mencionado na Solução 1.

O CA ARCserve Central Virtual Standby não pode se comunicar com o serviço web do CA ARCserve D2D em nós remotos

Válido em sistemas operacionais Windows.

Sintoma:

O CA ARCserve Central Virtual Standby não pode se comunicar com o serviço web do CA ARCserve D2D em nós remotos.

Solução:

A tabela a seguir descreve os motivos pelos quais o CA ARCserve Central Virtual Standby não pode se comunicar com o serviço web do CA ARCserve D2D em nós remotos e a ação corretiva correspondente:

Causa	Ação corretiva
A rede não está disponível ou não está estável ao aplicar diretivas.	Verifique se a rede está disponível e estável e tente novamente.
O computador do CA ARCserve D2D não pôde lidar com a carga quando o aplicativo tentou comunicar-se com o nó.	Verifique se a CPU no nó remoto do CA ARCserve D2D está em um estado normal e tente novamente.
O serviço do CA ARCserve D2D no nó remoto não estava em execução ao aplicar as diretivas.	Verifique se o nó remoto do CA ARCserve D2D está em execução e tente novamente.
O serviço do CA ARCserve D2D não está se comunicando adequadamente.	Reinicie este serviço do CA ARCserve D2D no nó remoto e tente novamente.

Erro de certificado é exibido ao efetuar logon no aplicativo

Válido em plataformas Windows.

Sintoma:

A seguinte mensagem é exibida na janela do navegador ao efetuar logon no aplicativo:

- Internet Explorer:

  `Há um problema com o certificado de segurança do site.`

- Firefox:

  `Esta conexão não é confiável.`

- Chrome:

  `O certificado de segurança do site não é confiável.`

Se você especificar uma opção que permita continuar com o site, será possível efetuar logon no aplicativo com êxito. No entanto, você encontrará este comportamento toda vez que efetuar logon no aplicativo.

Solução:

Este comportamento ocorre ao especificar o uso de HTTPS como o protocolo de comunicação. Para corrigir esse problema temporariamente, clique no link na janela do navegador que permite continuar com o site. No entanto, da próxima vez que você efetuar logon no aplicativo, você verá esta mensagem novamente.

O protocolo de comunicação HTTPS fornece um nível maior de segurança do que o protocolo de comunicação HTTP. Caso deseje continuar a se comunicar usando o protocolo de comunicação HTTPS, é possível adquirir um certificado de segurança do VeriSign e instalar o certificado no servidor do aplicativo. Como opção, é possível alterar o protocolo de comunicação usado pelo aplicativo para HTTP. Para alterar o protocolo de comunicação para HTTP, faça o seguinte:

1. Faça logon no servidor onde instalou o aplicativo.
2. Vá para o seguinte diretório:

   `C:\Arquivos de programas\CA\ARCserve Central Applications\BIN`

3. Execute o seguinte arquivo em lotes:

   `ChangeToHttp.bat`

4. após executar este arquivo, abra o Gerenciador de servidores do Windows.

   Reinicie o seguinte serviço:

   `Serviço do CA ARCserve Central Applications`

A mensagem Credenciais inválidas é exibida ao adicionar nós

Válido em plataformas Windows.

Sintoma:

A seguinte mensagem é exibida ao tentar adicionar nós para a tela Nós:

```
Credenciais inválidas.
```

Solução:

Este problema ocorre nas seguintes condições:

- As credenciais especificadas na caixa de diálogo Adicionar nós estão incorretas.
- O horário no nó não é o mesmo que o horário no servidor de aplicativos.

Para resolver esse problema, faça o seguinte:

1. Efetue logon no servidor do aplicativo e, em seguida, efetue logon no aplicativo.
2. Na página inicial, selecione Nó na Barra de navegação.

   A tela Nó é exibida.

3. Na barra de ferramentas Nó, clique em Adicionar e, em seguida, clique em Adicionar nó por IP/nome no menu pop-up.

   A caixa de diálogo Adicionar nó por IP/Nome é aberta.

4. Preencha os campos abaixo na caixa de diálogo Adicionar nó por do IP/Nome:
   - **IP/Nome do nó** - permite especificar o endereço IP ou o nome do nó.
   - **Descrição** - permite especificar uma descrição para o nó.
   - **Nome de usuário -** permite especificar o nome de usuário necessário para fazer logon no nó.
   - **Senha -** permite especificar a senha necessária para fazer logon no nó.

   Clique em Validar.

5. Se a mensagem Credenciais inválidas for exibida, faça o seguinte:
   a. Verifique se você especificou as credenciais corretas na caixa de diálogo Adicionar nós e clique em Validar.
   b. Se a mensagem Credenciais inválidas for exibida, verifique se o horário do sistema operacional no servidor de aplicativos é o mesmo que o do sistema operacional no nó.

      Observação: os horários do sistema operacional podem residir em diferentes fusos horários. No entanto, os horários do sistema operacional vezes não podem ser de datas diferentes. Verifique se a data do sistema operacional no nó não corresponde a mais de um dia calendário anterior ou posterior à data do sistema operacional no servidor do aplicativo.

Mensagens de credenciais inválidas no Windows XP

Válido em computadores que executam sistemas operacionais Windows XP.

Sintoma:

Ao adicionar nós com base no Windows XP pela tela Nó, a seguinte mensagem será exibida:

```
Credenciais de usuário inválidas.
```

Solução:

Sob várias condições, o Gerenciador do CA ARCserve Central Protection não pode adicionar nós com base no Windows XP com a opção de pasta Compartilhamento Simples de Arquivo do Windows especificada. Para resolver esse problema, faça o seguinte:

1. Efetue logon no nó do Windows XP e abra o Windows Explorer.
2. No menu Ferramentas, clique em Opções de pasta.

   A caixa de diálogo Opções de pasta é aberta.
3. Clique em Exibir e role até a opção Usar compartilhamento de arquivo simples (recomendável).
4. Limpar a marca de seleção de Usar compartilhamento de arquivo simples (recomendado) e clique em OK.

   O compartilhamento simples de arquivo está desativado.
5. Efetue logon no servidor do CA ARCserve Central Virtual Standby e, em seguida, adicione o nó.

Erros de acesso negado ocorrem ao adicionar um nó por IP/nome

Válido em todos os sistemas operacionais Windows com suporte ao UAC (User Account Control - Controle de Conta de Usuário).

Observação: o Windows Vista, o Windows Server 2008, o Windows Server 2008 R2 e o Windows 7 oferecem suporte ao UAC.

Sintoma:

Ao adicionar nós a partir da caixa de diálogo Adicionar nó por IP/nome usando uma nova conta de usuário do Windows que é integrante do grupo de administradores, a seguinte mensagem é exibida:

```
Acesso negado. Verifique se o usuário tem privilégio de administrador e se o acesso ao Registro remoto não está bloqueado por uma diretiva de segurança local da máquina adicionada.
```

O resultado disso é que você não pode adicionar o nó.

Solução:

Você pode esperar este comportamento quando o UAC está ativado em computadores executando o sistema operacional Windows com suporte ao UAC. O UAC é um recurso do Windows que permite apenas que a conta de administrador efetue logon no computador a partir de um local remoto. A solução para esse comportamento é executar as etapas a seguir:

Siga estas etapas:

1. Efetue logon no nó usando a conta de administrador.
2. Abra o Painel de Controle do Windows.
3. Abra Contas de Usuário.
4. Na tela Fazer alterações na conta de usuário, clique em Alterar configurações de Controle de Conta de Usuário e, em seguida, execute um dos seguintes procedimentos:
   - **Windows Vista e Windows Server 2008:** na tela Fazer alterações na conta de usuário, clique em Ativar ou desativar o Controle de Conta de Usuário. Em seguida, na tela Ativar o Controle de Conta de Usuário (UAC) para tornar o computador mais seguro, desmarque a caixa de seleção ao lado de Utilizar o Controle de Conta de Usuário (UAC) para ajudar a proteger o computador e clique em OK.

     Reinicie seu computador para aplicar as alterações ao UAC.
   - **Windows Server 2008 r2 e Windows 7:** na tela Definir quando deverá ser notificado sobre alterações no computador, mova o controle deslizante de Sempre notificar para Nunca notificar. Clique em OK e feche o Painel de controle do Windows.

     Reinicie seu computador para aplicar as alterações ao UAC.

5. Após a reinicialização do computador, verifique se as seguintes configurações foram aplicadas ao servidor do monitor e ao nó do CA ARCserve D2D ou ao sistema proxy de backup:
   - O serviço do Windows Server está em execução.
   - O serviço Compartilhamento de arquivo e impressora tem permissão para se comunicar através do firewall do Windows.
   - Quando o nó não é necessário para o ingresso em um domínio, o Serviço de logon de rede tem permissão para se comunicar através do firewall do Windows.
   - O valor de Diretiva de segurança local, Diretivas locais, Opções de segurança e Acesso à rede: modelo de compartilhamento e segurança para contas locais é Clássico.
6. Verifique se a seguinte configuração foi aplicada ao servidor do Modo de espera virtual:
   - O valor de Diretiva de segurança local, Diretivas locais, Opções de segurança e Segurança de rede: o nível de autenticação do LAN Manager é Enviar LM e NTLM - use a segurança da sessão NTLMv2, se estiver negociada.

Os nós não aparecem na tela Nó após alterar o nome do nó

Válido em plataformas Windows.

Sintoma:

O nome do host do nó foi alterado depois que ele foi adicionado à tela Nó. O nó não será mais exibido na tela Nó.

Solução:

Esse comportamento é esperado. O CA ARCserve Central Virtual Standby mantém o nome do nó que foi adicionado da tela Nó. Ao renomear o nó, o Virtual Standby poderá não detectá-lo. Do mesmo modo, o nó não será exibido na tela Nó.

Para exibir os nós renomeados na tela, proceda da seguinte maneira:

1. Renomeie o nó.
2. Abra a tela Nó e exclua o nó (na página 50) que foi renomeado.
3. Adicione o nó (na página 27) usando seu novo nome.

Ocorrem erros Sistema operacional não encontrado

Válido em plataformas Windows.

Sintoma:

A mensagem abaixo é exibida quando há falha ao ligar uma máquina no modo de espera virtual:

```
Sistema operacional não encontrado.
```

Solução:

Esse comportamento pode ocorrer em máquinas virtuais que contenham dispositivos SCSI e IDE. Se esse problema ocorrer, examine a maneira como os discos estão configurados na máquina virtual e verifique se a sequência de inicialização da máquina virtual recuperada é igual à da máquina virtual de origem. Se a sequência de inicialização for diferente, atualize o BIOS na máquina virtual recuperada para corresponder ao da origem.

Observação: use (0:1) para representar o primeiro disco IDE.

Falha em tarefas de modo de espera virtual para sistemas Hyper-V

Válido em sistemas operacionais Windows.

Sintoma:

Falha em tarefas de modo de espera virtual para sistemas Hyper-V. A seguinte mensagem é exibida no log de atividades:

```
Falha na tarefa do modo de espera virtual ao obter a VM do Hyper-V.
```

Solução:

Tarefas de modo de espera virtual nas seguintes condições:

- O serviço web de modo de espera virtual não consegue recuperar informações sobre a máquina virtual a partir do sistema Hyper-V. Os problemas de comunicação entre o sistema do servidor do CA ARCserve Central Virtual Standby e o do Hyper-V ocorrem quando os serviços do Hyper-V não estão em execução no sistema Hyper-V.

  Solução: certifique-se de que todos os devidos serviços do Hyper-V estejam em execução no sistema Hyper-V.

- O sistema Hyper-V não contém a quantidade suficiente de espaço livre em disco necessária para criar a máquina no modo de espera virtual ou para criar seu instantâneo.

  Solução: considere reconfigurar o sistema Hyper-V para liberar mais espaço no volume do sistema.

Observação: se você detectar outras possíveis causas, entre em contato com o suporte da CA Technologies.

Falha em tarefas no modo de espera virtual devido a erros internos

Válido em sistemas operacionais Windows.

Sintoma 1:

Falha nas tarefas do Virtual Standby. Uma das seguintes mensagens é exibida no log de atividades:

```
Falha ao converter o disco virtual
Erro interno, entre em contato com o suporte técnico
```

Além disso, o VDDK relata a seguinte mensagem de erro:

```
Erro desconhecido.
```

Solução 1:

Para resolver esse problema, considere as seguintes soluções:

- É possível haver falha em operações de conversão quando não há espaço suficiente no armazenamento de dados especificado na diretiva do Virtual Standby. O VDDK retorna a mensagem, pois a API do VDDK, no momento, não oferece suporte ao recurso para detectar a quantidade de espaço livre em disco no armazenamento de dados. Para corrigir o problema, libere a quantidade de espaço em disco no armazenamento de dados original necessária para que a operação seja concluída e, em seguida, envie a tarefa novamente.
- Interferências e excesso de tráfego na rede podem causar falha nas operações de conversão. Para corrigir o problema, certifique-se de que o sistema do nó de origem e do ESX Server ou vCenter Server possam se comunicar pela rede e, em seguida, reenvie a tarefa.

- Várias conexões simultâneas que consistem em tarefas de backup ou de recuperação via VM para o sistema ESX Server ou vCenter Server, que inclui as conexões SDK do vSphere por meio do cliente vSphere para VMware, podem provocar a falha das tarefas. Para corrigir este problema, feche todas as conexões desnecessárias e, em seguida, reenvie a tarefa.

  Este problema é o resultado de uma limitação de conexão do VDDK da VMware. Os limites do protocolo NFC (Network File Copy) a seguir se aplicam:

  - ESX 4: máximo de 9 conexões diretas
  - ESX 4 pelo vCenter Server: máximo de 27 conexões
  - ESXi 4: máximo de 11 conexões diretas
  - ESXi 4 pelo vCenter Server: máximo de 23 conexões
  - ESXi 5: limitado por um buffer de transferência para todas as conexões do NFC e impostas pelo host; a soma de todos os buffers de conexão do NFC para um host ESXi não pode exceder 32 MB. 52 conexões por meio do vCenter Server que inclui o limite por host.

  Observação: as conexões não podem ser compartilhadas entre discos. Os limites máximo não se aplicam a conexões SAN e HOTADD. Se o cliente NFC não for desligado corretamente, as conexões podem permanecer abertas por dez minutos.

- Examine as seções de tarefas e eventos do log do cliente VMware vSphere para descobrir erros internos de uma máquina virtual específica. Corrija os erros internos e, em seguida, reenvie a tarefa.

  Exemplo: outro aplicativo ou operação está usando o arquivo VMDK. Para corrigir o problema, libere o arquivo e reenvie a tarefa.

Sintoma 2:

Falha nas tarefas do Virtual Standby. Uma das seguintes mensagens é exibida no log de atividades:

```
Falha ao converter o disco virtual
Erro interno, entre em contato com o suporte técnico
```

Além disso, o VDDK relata a seguinte mensagem de erro:

```
Open vmdk failed with error File not found.
```

Solução 2:

Este problema poderá ocorrer nas seguintes condições:

- O VDDK não pôde processar um instantâneo corretamente.
- O VDDK não pôde excluir o instantâneo manualmente ou ele é interno para a máquina virtual.

Para corrigir esse problema, envie a tarefa novamente. Caso a tarefa falhe novamente, exclua a máquina virtual recuperada e envie a tarefa novamente.

Sintoma 3:

Falha nas tarefas do Virtual Standby. Uma das seguintes mensagens é exibida no log de atividades:

```
Falha ao converter o disco virtual
Erro interno, entre em contato com o suporte técnico
```

Além disso, o VDDK relata a seguinte mensagem de erro:

```
"Open vmdk failed" ou "The server refused connection"
```

Solução 3:

Este problema é o resultado de uma limitação de conexão do VDDK da VMware. Os limites do protocolo NFC (Network File Copy) a seguir se aplicam:

- ESX 4: máximo de 9 conexões diretas
- ESX 4 pelo vCenter Server: máximo de 27 conexões
- ESXi 4: máximo de 11 conexões diretas
- ESXi 4 pelo vCenter Server: máximo de 23 conexões

Observação: as conexões não podem ser compartilhadas entre discos. Os limites máximo não se aplicam a conexões SAN e HOTADD. Se o cliente NFC não for desligado corretamente, as conexões podem permanecer abertas por dez minutos.

Falha nas tarefas de modo de espera virtual usando o modo de transporte hotadd

Válido em plataformas Windows.

Sintoma:

As operações de recuperação falham ao recuperar dados usando o modo de transporte hotadd. A seguinte mensagem é exibida no log de atividades:

```
Ocorreu um erro desconhecido. Entre em contato com o Suporte técnico.
```

Além disso, o VDDK relata a seguinte mensagem de erro:

```
Erro desconhecido.
```

Solução:

As operações de recuperação falham ao usar o modo de transporte hotadd quando as configurações de disco não estiverem definidas corretamente.

Para configurar o disco, faça o seguinte:

1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.

   Abra a linha de comando do Windows.

2. Na linha de comando, execute o seguinte comando

   ```
   diskpart
   ```

   Pressione Enter.

   Digite SAN e, em seguida, pressione Enter.

   A diretiva atual da SAN é exibida.

3. Digite o seguinte comando:

   ```
   SAN POLICY = OnlineAll
   ```

   Pressione Enter.

   A diretiva da SAN está configurada para não montar automaticamente volumes hospedados pela SAN.

4. Para limpar o atributo de somente leitura do disco específico da SAN, selecione o disco a partir da lista de discos e digite o seguinte comando:

   ```
   attribute disk clear readonly
   ```

   Pressione Enter.

5. Digite exit e, em seguida, pressione Enter.

O disco está configurado e é possível enviar a tarefa novamente. Se a tarefa falhar novamente, monte os discos hotadd manualmente usando o gerenciamento de discos no sistema proxy.

Para montar os discos manualmente, faça o seguinte:

1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.

   Abra o Painel de Controle do Windows e clique duas vezes em Ferramentas Administrativas.

   A janela Ferramentas Administrativas é exibida.

2. Na lista Favoritos, clique duas vezes em Gerenciamento do Computador.

   O Gerenciamento do computador é exibido.

3. Expanda Armazenamento e clique em Gerenciamento de Disco.

   Os discos são exibidos.

4. Clique com o botão direito no disco que deseja montar e clique em Online.

   O disco está montado e é possível enviar a tarefa novamente.

As tarefas no modo de espera virtual terminam sem mensagens de aviso para as sessões

Válido em plataformas Windows.

Sintoma:

As tarefas de modo de espera virtual terminam, e uma das seguintes mensagens são exibidas no log de atividades:

```
Virtual Standby job ends with no session(s).
```

```
O Modo de espera virtual não pôde detectar as sessões de backup no servidor do CA ARCserve D2D para criar instantâneos do ponto de recuperação. É possível que não haja nenhuma sessão de backup no servidor do CA ARCserve D2D para conversão.
```

Solução:

Você encontrará problemas desse tipo nas seguintes condições:

- Você usou o Gerenciador do CA ARCserve Central Protection para aplicar a diretiva de backup do CA ARCserve D2D ao nó e a uma das opções abaixo.

  – As configurações da origem do backup do CA ARCserve D2D foram alteradas da opção Select individual volumes to back up para a opção Back up the entire machine, e um backup completo não foi enviado ou não foi concluído usando as configurações de backup atualizadas depois que a diretiva de modo de espera virtual foi implantada no nó.

    Solução: enviar um backup completo do nó do CA ARCserve D2D.

  – As configurações da origem do backup do CA ARCserve D2D foram alteradas da opção Back up the entire machine para a opção Select individual volumes to back up depois que a diretiva de modo de espera virtual foi implantada no nó.

    Solução: altere as configurações da origem do backup do CA ARCserve D2D da opção Select individual volumes to back up para a opção Back up the entire machine e, em seguida, envie um backup completo do nó do CA ARCserve D2D.

As tarefas de backup e recuperação não usam o modo de transporte da SAN.

Válido em plataformas Windows.

Sintoma:

As tarefas de backup e recuperação não usam o modo de transporte da SAN (na página 215). As tarefas são revertidas para o modo de transporte NDB (na página 215) ou o modo de transporte NBDSSL (na página 215). O campo Transport Mode, na caixa de diálogo Backup Status Monitor, exibe o modo usado.

Solução:

Os sintomas descritos acima podem ocorrer quando o LUN da SAN não está configurado corretamente no sistema proxy do backup. No entanto, se o Gerenciamento de disco do Windows detectar o LUN da SAN e o problema persistir, o disco pode estar offline ou o atributo de leitura do disco não está correto. Para evitar esse comportamento, reconfigure o disco.

Para configurar o disco, faça o seguinte:

1. Efetue logon no nó de origem ou no servidor de monitoramento usando uma conta com privilégios administrativos.
2. Abra a linha de comando do Windows.
3. Na linha de comando, execute o seguinte comando

   ```
   diskpart
   ```

   Pressione Enter.
4. Digite SAN e, em seguida, pressione Enter.

   A diretiva atual da SAN é exibida.
5. Digite o seguinte comando:

   ```
   SAN POLICY = OnlineAll
   ```

   Pressione Enter.

   A diretiva da SAN está configurada para não montar automaticamente volumes hospedados pela SAN.

6. Para limpar o atributo de somente leitura do disco específico da SAN, selecione o disco a partir da lista de discos e digite o seguinte comando:

   ```
   attribute disk clear readonly
   ```

   Pressione Enter.

7. Digite exit e, em seguida, pressione Enter.

O disco está configurado e é possível enviar a tarefa novamente.

Não é possível montar discos com tarefas de backup e recuperação usando o modo de transporte hotadd

Válido em plataformas Windows.

Sintoma:

As tarefas de backup e recuperação que usam o modo de transporte hotadd não podem montar discos no nó de origem ou no servidor de monitoramento. Além disso, a seguinte mensagem é exibida no log de atividades:

```
Falha ao abrir o arquivo VMDK %1!s!. Consulte o log de depuração AFBackend.Log para obter mais detalhes. Entre em contato com o Suporte técnico.
```

Solução:

Para resolver esse problema, faça o seguinte:

1. Abra o VMware vSphere Client.

   Efetue logon no sistema do ESX Server ou vCenter Server usando credenciais administrativas.

2. Selecione a máquina virtual do proxy e edite suas configurações.
3. Remover os discos hotadd do sistema proxy, caso tenham sido conectados durante a tarefa de conversão.
4. Envie a tarefa novamente.

Número do erro na Solução de problemas

A tabela a seguir descreve o números do erro exibido como mensagens pop-up ao adicionar ou atualizar nós usando o CA ARCserve Central Virtual Standby.

Número do erro	Descrição	Solução possível
12884901933	Não é possível estabelecer conexão com o serviço do CA ARCserve D2D em *** e número do erro é 12884901933. Verifique se todas as entradas para o nó estão corretas e se o serviço do CA ARCserve D2D está em execução.	Verifique o seguinte: ■ O serviço do CA ARCserve D2D está em execução no nó. ■ O nome do host, o endereço IP e o protocolo de comunicação especificados para o nó estão correto. ■ O serviço web do CA ARCserve D2D no nó está em execução, e não aparece bloqueado devido ao fato do DNS conseguir resolver o endereço IP do nó. ■ O serviço web do CA ARCserve D2D no nó está em execução, e o firewall do Windows, ou qualquer outro firewall não está bloqueando a comunicação. ■ O cabo de rede está conectado e o nó está funcionando corretamente. ■ O usuário conectado ao nó tem as permissões necessárias para se comunicar usando uma rede sem fio.

O link Adicionar nova guia não é iniciado corretamente no Internet Explorer 8 e 9 nem no Chrome

Válido no Windows

Sintoma:

Ao adicionar o link de uma nova guia à barra de navegação especificando o URL de um HTTPS, as seguintes mensagens de erros serão exibidas quando eu clicar na nova guia:

- Internet Explorer 8 e 9:

  ```
  O conteúdo foi bloqueado porque não foi assinado por um certificado de segurança válido.
  ```

- Chrome:

  ```
  Esta página web não está disponível.
  ```

Solução:

Para corrigir esse problema no Internet Explorer, faça o seguinte:

- Internet Explorer 8:

  Clique na barra de mensagens e selecione "Exibir Conteúdo Bloqueado".

- Internet Explorer 9:

  Clique no botão "Mostrar conteúdo" na barra de mensagens na parte inferior da página. A página é atualizada e o link para a guia adicionada é aberto com êxito.

Para corrigir esse problema no Chrome, execute as seguintes etapas:

Etapa 1 - Exportar certificado:

1. Abra uma nova guia no Chrome e digite o URL do HTTPS.

   A mensagem de aviso "The site's security certificate is not trusted!" é exibida.

2. Na barra de endereços, clique no cadeado com 'X'.

   Uma janela pop-up é exibida com o link Certification Information.

3. Clique nesse link.

   A caixa de diálogo Certificate é aberta.

4. Clique na guia Details e, em seguida, clique em Copy to File, para salvar o certificado em seu computador local.

   A caixa de diálogo do Assistente para exportação de certificados é exibida.

5. Clique em Next para selecionar o formato deseja usar para exportar o arquivo.

   Observação: o binário X.509 codificado por DER (*.CER) vem selecionado por padrão.

6. Clique em Next para ir para o local em que deseja salvar o certificado.
7. Clique em Next para concluir o Certificate Export Wizard e, em seguida, clique em Finish.

O certificado é exportado com êxito.

Etapa 2 - Importar certificado:

1. Abra a caixa de diálogo Tools Options no Chrome.

   A tela Options é aberta.

2. Selecione a opção Under the Hood e clique em Manage Certificates from HTTPS/SSL.

   A caixa de diálogo Certificates é aberta.

3. Clique em Importar.

   A caixa de diálogo do Assistente para importação de certificados é exibida.

4. Clique em Next para ir para o certificado salvo no seu computador local.
5. Clique em Avançar para abrir o Armazenamento de certificados.

   A caixa de diálogo Certificate Store é aberta.

6. Clique em Browse para abrir a caixa de diálogo Select Certificate Store.

   A caixa de diálogo Select Certificate Store é aberta.

7. Selecione as Trusted Root Certification Authorities na lista de arquivos e clique em OK.

   A caixa de diálogo Armazenamento de certificados é aberta.

8. Clique em Next para concluir o Certificate Import Wizard e, em seguida, clique em Finish.

   A caixa de diálogo Security Warning é exibida, indicando que você está prestes a instalar um certificado.

   Clique em Sim para concordar com os termos.

O certificado é importado com êxito.

O link Adicionar nova guia, os feeds de RSS e os comentários de rede social não são iniciados corretamente no Internet Explorer 8 e 9

Válido no Windows

Sintoma:

Para o URL de um HTTPS do CA ARCserve Central Applications:

Ao adicionar o link de uma nova guia à barra de navegação especificando o URL de um HTTP, as seguintes mensagens de erro serão exibidas quando eu clicar na nova guia e no link Comentários:

```
A navegação para a página da web foi cancelada.
```

Além disso, os feeds de RSS não são exibidos.

Observação: o link Comentários também exibe a mensagem de erro, mesmo que você não selecione o link da nova guia.

Solução:

Para resolver esse problema, faça o seguinte:

- Internet Explorer 8:

  Após efetuar logon, clique em Não na mensagem pop-up de aviso de segurança, "Deseja exibir apenas o conteúdo oferecido de forma segura por esta página da Web?". Clicar em Não permite a entrega de conteúdo que não seja seguro em sua página da web.

- Internet Explorer 9:

  Clique no botão "Mostrar todo o conteúdo" na barra de mensagens na parte inferior da página. A página é atualizada e o link da guia adicionada é aberto com êxito.

Não é possível especificar um asterisco ou caractere sublinhado como um caractere curinga nos campos do filtro usando um teclado japonês

Válido no Windows

Sintoma:

Devido à diferença entre o teclado dos EUA e o japonês, não é possível digitar o caractere curinga "*" e outros caracteres especiais no teclado japonês, como o caractere sublinhado "_", nos campos de filtro a seguir:

- Ocorre apenas no Firefox:
  - Nó > Adicionar grupo - campo Filtragem pelo nome do nó
  - Políticas > guia Atribuição de diretiva > Diretiva a ser atribuída ou ter a atribuição cancelada - campo Filtragem pelo nome do nó
  - Restaurar > Explorador de nós - campo Nome do nó

Solução:

- Para evitar que isso ocorra, abra um aplicativo de edição de texto, como o Bloco de notas. Digite os caracteres especiais, como "*" e "_", no editor de texto. Em seguida, copie os caracteres do editor de texto no campo.

Máquinas virtuais não ligam automaticamente

Válido no Windows.

Sintoma:

As máquinas virtuais não ligam automaticamente. O valor de Recuperação, Configurações de substituição é definido como Iniciar a máquina virtual automaticamente.

Solução:

Esse comportamento é esperado. O aplicativo não consegue ligar automaticamente máquinas virtuais que foram adicionadas de servidores do CA ARCserve Central Host-Based VM Backup. Como resultado, quando você implanta diretivas que contêm um método de recuperação definido como Iniciar a máquina virtual automaticamente para nós protegidos pelo Host-Based VM Backup, o Virtual Standby altera o valor do método de recuperação para Iniciar a máquina virtual manualmente.

A solução para esse comportamento é proteger a máquina virtual usando o CA ARCserve D2D ou o Gerenciador do CA ARCserve Central Protection.

Capítulo 6: Aplicando práticas recomendadas

Esta seção contém os seguintes tópicos:

Como o processo de instalação afeta os sistemas operacionais

O processo de instalação do CA ARCserve Central Applications atualiza vários componentes do sistema operacional Windows, usando um mecanismo de instalação denominado MSI (Microsoft Installer Package). Os componentes incluídos no MSI permitem que o CA ARCserve Central Applications execute ações personalizadas para instalação, atualização e desinstalação do CA ARCserve Central Applications.

A tabela a seguir descreve as ações personalizadas e os componentes afetados:

Observação: todos os pacotes MSI do CA ARCserve Central Applications chamam os componentes relacionados nesta tabela quando você instala e desinstala o CA ARCserve Central Applications.

Componente	Descrição
CallAllowInstall	Permite ao processo de instalação verificar condições relativas à instalação atual do CA ARCserve Central Applications.
CallPreInstall	Permite ao processo de instalação ler e gravar propriedades do MSI. Por exemplo, ler o caminho de instalação do CA ARCserve Central Applications no MSI.
CallPostInstall	Permite ao processo de instalação executar várias tarefas relativas à instalação. Por exemplo, registrar o CA ARCserve Central Applications no Registro do Windows.
CallAllowUninstall	Permite ao processo de desinstalação verificar condições relativas à instalação atual do CA ARCserve Central Applications.
CallPreUninstall	Permite ao processo de desinstalação executar várias tarefas relativas à desinstalação. Por exemplo, cancelar o registro do CA ARCserve Central Applications no Registro do Windows.

Componente	Descrição
CallPostUninstall	Permite que o processo de desinstalação execute várias tarefas depois de desinstalar os arquivos instalados. Por exemplo, a remoção dos arquivos restantes.
ShowMsiLog	Exibe o arquivo de log do Windows Installer no Bloco de notas, caso o usuário final marque a caixa de seleção Mostrar log do Windows Installer nas caixas de diálogo SetupCompleteSuccess, SetupCompleteError ou SetupInterrupted e, em seguida, clique em Concluir. (Funciona somente com o Windows Installer 4.0.)
ISPrint	Imprime o conteúdo de um controle ScrollableText em uma caixa de diálogo. Essa é uma ação .dll personalizada do Windows Installer. O nome do arquivo .dll é SetAllUsers.dll e seu ponto de entrada é PrintScrollableText.
CheckForProductUpdates	Usa o FLEXnet Connect para verificar a existência de atualizações do produto. Essa ação personalizada abre um arquivo executável chamado Agent.exe, que transmite o seguinte: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Usa o FLEXnet Connect para verificar a existência de atualizações do produto ao reinicializar. Essa ação personalizada abre um arquivo executável chamado Agent.exe, que transmite o seguinte: /au[ProductCode] /EndOfInstall /Reboot

- **Diretórios atualizados -** o processo de instalação instala e atualiza arquivos do CA ARCserve Central Applications nos seguintes diretórios, por padrão:

  `C:\Arquivos de programas\CA\ARCserve Central Applications\BIN`

  É possível instalar o CA ARCserve Central Applications no diretório de instalação padrão ou em um diretório diferente. O processo de instalação copia vários arquivos de sistema para o seguinte diretório:

  `C:\WINDOWS\SYSTEM32`

- **Chaves de registro do Windows atualizadas--**o processo de instalação atualiza as chaves de registro do Windows a seguir:

  Chaves padrão do Registro:

  `HKLM\SOFTWARE\CA\CA ARCserve Central Applications`

  O processo de instalação cria chaves de registro e modifica várias outras chaves de registro, de acordo a configuração atual do sistema.

- **Aplicativos instalados**--o processo de instalação inclui estes aplicativos em seu computador:
  - Licenciamento CA
  - Microsoft Visual C++ 2005 SP1 redistribuível
  - Microsoft Windows Installer 3.1 Redistributable (v2) Package
  - JRE (Java Runtime Environment) 1.6.0_16
  - Tomcat 6.0.32

Arquivos binários contendo informações incorretas sobre a versão do arquivo

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications, os quais contém informações incorretas sobre a versão do arquivo. A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
UpdateData.exe	Licença da CA
zlib1.dll	Biblioteca de compactação zlib

Arquivos binários que não contêm um manifesto incorporado

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications, os quais não contêm um manifesto incorporado nem em texto. A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
BaseLicInst.exe	Licença da CA
UpdateData.exe	Licença da CA
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

Arquivos binários cujo nível de privilégio exige acesso de administrador ao manifesto

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications com um nível de privilégio de administrador ou o mais alto disponível. É preciso efetuar logon usando uma conta administrativa ou uma conta com o nível de permissão mais alto disponível para executar diversos serviços, componentes e aplicativos do CA ARCserve Central Applications. Os binários correspondentes contêm funcionalidades específicas do CA ARCserve Central Applications, não disponíveis para uma conta de usuário básica. Assim, o Windows solicitará que você confirme uma operação especificando sua senha ou usando uma conta com privilégios administrativos para concluí-la.

- **Privilégios administrativos** - o perfil administrativo ou uma conta com privilégios administrativos têm permissões de leitura, gravação e execução para todos os recursos do Windows e do sistema. Caso não tenha privilégios administrativos, você será solicitado a digitar o nome de usuário e a senha de um usuário administrador para continuar.
- **Privilégios mais altos disponíveis** - uma conta com os privilégios mais altos disponíveis é uma conta de usuário básica e uma conta de usuário avançado que opera com privilégios administrativos.

A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications

Nome do arquivo binário	Origem
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Como o licenciamento do CA ARCserve Central Virtual Standby funciona

O CA ARCserve Central Virtual Standby contém as seguintes licenças:

- CA ARCserve Central Virtual Standby-Físico
- CA ARCserve Central Virtual Standby-VMware
- CA ARCserve Central Virtual Standby-Hyper-V

Todas as licenças são com base na contagem. O CA ARCserve Central Virtual Standby verifica e concede licenças para os nós do CA ARCserve D2D com base nos seguintes critérios:

- O CA ARCserve Central Virtual Standby aplica as licenças do CA ARCserve Central Virtual Standby-Físico a todos os nós do CA ARCserve D2D que você adicionar por Nome/endereço IP ou importar de um arquivo. O CA ARCserve Central Virtual Standby concede licenças do CA ARCserve Central Virtual Standby-Físico aos nós após você aplicar uma diretiva aos nós virtuais e iniciar o processo de conversão virtual.

  Observação: este é o comportamento padrão para o licenciamento do CA ARCserve Central Virtual Standby.

- O CA ARCserve Central Virtual Standby aplica as licenças do CA ARCserve Central Virtual Standby-VMware a todos os nós do CA ARCserve D2D que você adicionar por Nome/endereço IP ou importar de um arquivo e as máquinas virtuais que residirem em sistemas ESX Server ou vCenter Server. No entanto, antes que o CA ARCserve Central Virtual Standby possa aplicar licenças do CA ARCserve Central Virtual Standby-VMware aos nós, é necessário associá-los a um determinado sistema ESX Server ou vCenter Server.

  Observação: para obter mais informações, consulte Especificar o sistema ESX Server ou vCenter Server para nós do VMware (na página 29).

  O CA ARCserve Central Virtual Standby concede as licenças do CA ARCserve Central Virtual Standby-VMware para cada sistema ESX Server após aplicar uma diretiva aos nós virtuais e iniciar o processo de conversão.

- O CA ARCserve Central Virtual Standby aplica as licenças do CA ARCserve Central Virtual Standby-VMware a todos os nós da máquina virtual que você importar de um sistema do CA ARCserve Central Host-Based VM Backup. O CA ARCserve Central Virtual Standby concede as licenças do CA ARCserve Central Virtual Standby-VMware para os nós da máquina virtual após aplicar uma diretiva aos nós e iniciar o processo de conversão virtual.
- O CA ARCserve Central Virtual Standby aplica as licenças do CA ARCserve Central Virtual Standby-Hyper-V a todos os nós do CA ARCserve D2D que você adicionar por Nome/endereço IP ou importar de um arquivo e que residir no hypervisor do Hyper-V. O CA ARCserve Central Virtual Standby detecta a presença do servidor Hyper-V quando você adiciona por meio dos nós por Nome/endereço IP ou importa os nós a partir de um arquivo. O CA ARCserve Central Virtual Standby concede as licenças do CA ARCserve Central Virtual Standby-Hyper-V aos nós do <caader> depois que você adicionar os nós por Nome/endereço IP ou importar os nós a partir de um arquivo.

Contagem do mecanismo

A tabela a seguir descreve a quantidade de licenças do CA ARCserve Central Virtual Standby necessárias para um determinado cenário.

Tipo de nó do D2D	Licença necessária	Contagem do mecanismo
Nó físico	CA ARCserve Central Virtual Standby-Físico	Uma licença para cada nó
Máquina virtual VMware	CA ARCserve Central Virtual Standby-VMware	Uma licença para cada sistema ESX/vCenter Server
Máquina virtual Hyper-V	CA ARCserve Central Virtual Standby-Hyper-V	Uma licença para cada sistema Hyper-V

Exemplos

- O CA ARCserve Central Virtual Standby está protegendo cinco nós físicos do CA ARCserve D2D. Cinco licenças do CA ARCserve Central Virtual Standby-Físico são necessárias.
- O CA ARCserve Central Virtual Standby está protegendo três máquinas virtuais VMware que residem em um sistema ESX Server. Uma licença do CA ARCserve Central Virtual Standby-VMware é necessária.
- O CA ARCserve Central Virtual Standby está protegendo 100 máquinas virtuais VMware distribuídas em um sistema ESX Server. Dez licenças do CA ARCserve Central Virtual Standby-VMware são necessárias.
- O CA ARCserve Central Virtual Standby está protegendo 20 máquinas virtuais Hyper-V distribuídas em cinco sistemas Hyper-V Server. Cinco licenças do CA ARCserve Central Virtual Standby-Hyper-V são necessárias.

- O CA ARCserve Central Virtual Standby está protegendo três máquinas virtuais do Hyper-V que residem em um sistema Hyper-V e três máquinas virtuais do VMware que residem no sistema ESX Server. Uma licença do CA ARCserve Central Virtual Standby-VMware é necessária e uma licença do CA ARCserve Central Virtual Standby-Hyper-V também é necessária.
- O CA ARCserve Central Virtual Standby está protegendo cinco máquinas virtuais VMware importadas do CA ARCserve Central Host-Based VM Backup que residem em um sistema ESX Server. Uma licença do CA ARCserve Central Virtual Standby-VMware é necessária.

Glossário

Conversão virtual

A conversão virtual é o processo em que o CA ARCserve Central Virtual Standby converte pontos de recuperação do CA ARCserve D2D de nós de origem para arquivos de dados da máquina virtual, denominados instantâneos de pontos de recuperação.

Diretivas

Uma diretiva é um conjunto de especificações para proteger um nó em um ou mais CA ARCserve Central Applications.

Grupo de nós

Um nó de grupo é um método pelo qual todos os nós gerenciados por um ou mais CA ARCserve Central Applications podem ser organizados por finalidade, por SO ou por aplicativos instalados.

Instantâneo do ponto de recuperação

Um instantâneo do ponto de recuperação é um arquivo VMDK (VMware Virtual Disk) ou VHD (Microsoft Virtual Hard Disk) que o CA ARCserve Central Virtual Standby cria a partir dos pontos de recuperação do CA ARCserve D2D. O CA ARCserve Central Virtual Standby permite ligar máquinas virtuais usando os instantâneos de ponto de recuperação quando há falha nos servidores de origem em execução no CA ARCserve D2D que estiverem no seu ambiente de produção.

Modo de transporte HOTADD

O modo de transporte HOTADD é um método de transporte de dados que permite fazer backup de máquinas virtuais configuradas com discos SCSI. Para obter mais informações, consulte o Guia de Programação da API do disco virtual no site do VMware.

Modo de transporte NBD

O modo de transporte NBD, também conhecido como modo de transporte LAN, usa o protocolo NFC (Network File Copy - Cópia de arquivos de rede) para estabelecer comunicação. Várias operações do VDDK e VCB usam uma conexão para cada disco virtual acessado em cada host ESX/ESXi Server ao usar o NDB.

Modo de transporte NBDSSL

O modo de transporte NBDSSL (Network Block Device Secure Sockets Layer) usa o protocolo NFC (Network File Copy) para se comunicar. O NBDSSL transfere dados criptografados usando redes de comunicação TCP/IP.

Modo de transporte SAN

O modo de transporte SAN (Storage Area Network) permite a transferência de dados de backup de sistemas proxy conectados à SAN para armazenar dispositivos por meio de comunicação Fibre Channel.

Nó

O nó é uma máquina física ou virtual gerenciada por um ou mais CA ARCserve Central Applications.

Ponto de recuperação

Um ponto de recuperação é uma imagem de backup de blocos de pai mais filho mais antigo. Os backups s filhos ão mesclados com o backup pai para criar novas imagens de ponto de recuperação para que o valor especificado seja sempre mantido.

Servidor de monitoramento

Um servidor de monitoramento é um servidor que verifica o status dos servidores de origem em ambientes do CA ARCserve Central Virtual Standby.

Sinal de monitoramento

Um sinal de monitoramento é um sinal que os nós de origem enviam para os servidores de monitoramento identificar o status do nó.

Índice remissivo

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V